Available online at www.sciencedirect.com

SCIENCE DIRECT®

Information and Computation 196 (2005) 71–94

Information and Computation

www.elsevier.com/locate/ic

# Lower bounds on systolic gossip☆

Michele Flammini[a,*], Stéphane Pérennès[b]

[a] *Dipartimento di Informatica, Università di L'Aquila, via Vetoio Loc.Coppito, I-67100 L'Aquila, Italy*

[b] *MASCOTTE Project I3S-CNRS/Université de Nice–Sophia Antipolis/INRIA, 2004 Route des Lucioles, BP 93, F-06902 Sophia-Antipolis Cedex, France*

Received 29 November 1998; revised 9 June 2000

**Abstract**

Gossiping is an extensively investigated information dissemination process in which each processor has a distinct item of information and has to collect all the items possessed by the other processors. In this paper, we provide an innovative and general lower bound technique relying on the novel notion of delay digraph of a gossiping protocol and on the use of matrix norm methods. Such a technique is very powerful and allows the determination of new and significantly improved lower bounds in many cases. In fact, we derive the first general lower bound on the gossiping time of systolic protocols, i.e., constituted by a periodic repetition of simple communication steps. In particular, given any network of $n$ processors and any systolic period $s$, in the directed and the undirected half-duplex cases every $s$-systolic gossip protocol takes at least $\log(n)/\log(1/\lambda) - O(\log\log(n))$ time steps, where $\lambda$ is the unique solution between 0 and 1 of $\lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)} = 1$, with $p_i(\lambda) = 1 + \lambda^2 + \cdots + \lambda^{2i-2}$ for any integer $i > 0$. We then provide improved lower bounds in the directed and half-duplex cases for many well-known network topologies, such as Butterfly, de Bruijn and Kautz graphs. All the results are extended also to the full-duplex case. Our technique is very general, as for $s \to \infty$ it allows the determination of improved results even for non-systolic protocols. In fact, for general networks, as a simple corollary it yields a lower bound only an $O(\log\log(n))$ additive factor

☆ This work was supported by the Future and Emerging Technologies programme of the EU under contract number IST-1999-14186 (ALCOM-FT), by the EU RTN project ARACNE, by the EU TMR Research Training Grant No. ERB-FMBICT960861, by the Italian "Progetto Cofinanziato: Resource Allocation in Computer Networks" and by the Italian CNR Project "Young."

* Corresponding author. Fax: +39 0862 433 057.

*E-mail addresses:* flammini@di.univaq.it (M. Flammini), speren@sophia.inria.fr (S. Pérennès).



doi:10.1016/j.ic.2004.09.002

far from the general one independently proved in [Proc. 1st ACM Symposium on Parallel Algorithms and Architectures (SPAA), 1989, p. 318; Topics in Combinatorics and Graph Theory (1990) 451; SIAM Journal on Computing 21(1) (1992) 111; Discrete Applied Mathematics 42 (1993) 75] for all graphs and any (non-systolic) gossip protocol. Moreover, for specific networks, it significantly improves with respect to the previously known results, even in the full-duplex case. Correspondingly, better lower bounds on the gossiping time of non-systolic protocols are determined in the directed, half-duplex and full-duplex cases for Butterfly, de Bruijn and Kautz graphs. Even if in this paper we give only a limited number of examples, our technique has wide applicability and gives a general framework that often allows to get improved lower bounds on the gossiping time of systolic and non-systolic protocols in the directed, half-duplex and full-duplex cases.


## 1. Introduction

Gossiping is an all-to-all information dissemination problem in which a distinct item originating at each processor of the network must be distributed to all the other processors. This is accomplished by means of a sequence of simple *communication rounds*, each specifying a set of active communication links that can be used by the corresponding incident processors to exchange the possessed items of information.

The gossiping problem has been extensively investigated in recent years for many different networks and under a large variety of models. A survey of the main related results can be found in [7,6,8,3,9,10,12].

In this paper, we consider the fundamental and most studied model, called whispering or processor-bound, where at each communication round each processor can have only one active incident link, i.e., the set of the active links forms a matching. If the network can be modeled as an undirected graph, it is possible to further distinguish between two different cases: the half-duplex mode, in which active links allow the transmission of messages only in one direction, and the full-duplex mode, in which messages can travel in both directions simultaneously.

We will consider particular gossiping strategies called "periodic" in [20,21,18] and "systolic" (or "traffic-light") in [8,14]. The main motivation behind these concepts correspond to the idea of Kung [16] who has introduced so-called "systolic computations" as parallel computations with cheap realization due to a very regular, synchronized periodic behavior of all processors of the interconnection network during the whole execution of the computation. Liestman and Richards [20] were the first who considered a very regular form of communication algorithms for broadcasting (one-to-many dissemination strategy) and gossiping. This form, later called "periodic" in [18], was based on the edge coloring of the graph underlying the network and on the periodic (cyclic) execution of communications rounds, each activating the links corresponding to the same color. A little more general concept was given in [8], where $s$-systolic communication algorithms correspond to a repetition of a given sequence of $s$ communication rounds. While broadcasting strategies can be systolized at no cost [8], this is in general not true for gossiping. The basic problem with systolic strategies remarked in [8] is how much must be paid for the systolization of gossiping protocols in concrete interconnection networks, i.e., what is the difference between the complexity of gossip and systolic gossip. In [8] optimal systolic protocols are given for paths and complete $d$-ary trees and it is shown that in the half-duplex mode the complexity of systolic gossip for paths is strictly higher

than normal gossip. In [20,14] systolic strategies are proposed for two-dimensional grids optimal up to a constant additive factor, but only for the full-duplex case. These results are improved in [11] by the introduction of optimal systolic algorithms both in the half and full-duplex cases. In [11] the authors present also optimal results for cycles in the half-duplex mode.

Concerning lower bounds on gossiping, denoted as $g(G)$ the gossiping time of a graph $G$, in the half-duplex mode it has been proved that $g(G) \geqslant 1.4404 \log(n)$ (from now on all logarithms are assumed to base 2) for all graphs $G$ of $n$ vertices [4,17,15,26], this bound being attained for complete graphs.

However, apart from the cases mentioned above, in general the best lower bounds for systolic gossiping are not better than those that can be inferred from broadcasting. Unfortunately, often this holds also for non-systolic gossiping.

The best lower bounds on the broadcasting time are as follows. Let the parameter $d$ be defined for undirected graphs as the maximum degree minus one and for directed graphs as the maximum out-degree. Then for bounded-degree networks in [22,2] it has been proved that the broadcasting time $b(G)$ of a graph $G$ of $n$ vertices with parameter $d$ satisfies $b(G) \geqslant c(d) \log(n)$, where $c(2) = 1.4404$, $c(3) = 1.1374$, $c(4) = 1.0562$ and for large $d$, $c(d) \approx (1 + \log(e)/2^d)$.

For Butterfly and de Bruijn networks better lower bounds have been obtained by using their structure in [13] and then improved in [23,24]. For example in [23] it is proved that for undirected Wrapped Butterflies $b(WBF(2, D)) \geqslant 1.7621D$ ($\approx 1.7621 \log(n)$) and $b(WBF(3, D)) \geqslant 2.0002D$ ($\approx 1.2619 \log(n)$), while for undirected de Bruijn networks $b(DB(2, D)) \geqslant 1.4404D$ ($= 1.4404 \log(n)$) and $b(DB(3, D)) \geqslant 1.8028D$ ($= 1.1374 \log(n)$).

Concerning upper bounds on the gossiping time for Butterfly and de Bruijn networks, in the half-duplex mode it has been proved that $g(WBF(2, D)) \leqslant 2.5 \log(n) + O(\sqrt{2 \log(n)})$ [9] and $g(DB(2, D)) \leqslant 3 \log(n) + 3$ [25]. These results have been improved in [24] by showing that in the systolic mode, for small constant period $s$, $g(WBF(2, D)) \leqslant 2.5 \log(n) + O(\sqrt{\log(n)})$ and $g(DB(2, D)) \leqslant 2 \log(n) + O(\sqrt{\log(n)})$.

In this paper, we provide an innovative and powerful lower bound technique relying on two different concepts: the novel notion in the field of delay digraph of a dissemination protocol and the use of matrix norm methods similar to those in [4,17,15,26]. The former allows to infer nice properties on the delays encountered while crossing two successive arcs, the latter permits to exploit well-know matrix properties in the estimation of the lower bounds. To the best of our knowledge this is the first technique combining such different aspects in a unified approach, as all the previous lower bound methods and results were based on classical graph combinatorial and information theoretical tools and/or deeply exploited the structural properties of the considered networks. Our technique allows in a surprising number of cases the determination of lower bounds that are at least as good or significantly improve with respect to the existing ones. Even if in this paper we give a limited number of examples, it has wide applicability and gives a general framework that often provides improved lower bounds by simply exploiting very general topological properties.

Concerning the shown results, we prove the first general lower bound on the gossiping time of systolic protocols for directed networks and undirected networks in the half-duplex mode. In particular, if we denote by $n$ the number of processors in the network, then any $s$-systolic gossip protocol takes at least $e(s) \log(n) - O(\log \log(n))$ time steps, where $e(s) = 1/\log(1/\lambda)$ and $\lambda$ is such that $0 < \lambda < 1$ and $\lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)} = 1$, with $p_i(\lambda) = 1 + \lambda^2 + \cdots + \lambda^{2i-2}$ for any integer $i > 0$. For $s = 3, 4, 5, 6, 7, 8$, this gives $e(3) = 2.8808$, $e(4) = 1.8133$, $e(5) = 1.6502$, $e(6) = 1.5363$, $e(7) = 1.5021$, and $e(8) = 1.4721$.

Our technique can be applied also to the full-duplex mode. However, in the general case, we obtain nearly the same lower bounds that come directly from broadcasting [22,2], i.e., differing only $O(\log\log(n))$. This is actually not due to a limit of our technique. In fact, recently in [5] it has been proved that all our results (in the directed, half-duplex and full-duplex modes) are optimal. Namely, for any systolic period $s$, there exist networks whose gossiping time differs only $O(\log\log(n))$ from the corresponding lower bound.

If more information about the network topology is known, finer lower bounds can be determined for many relevant interconnection networks, even for full-duplex protocols. Significantly improved results are thus provided in the directed, half-duplex and full-duplex cases for Butterflies, Wrapped Butterflies, de Bruijn and Kautz networks. For example, as a direct comparison with the half-duplex upper bounds mentioned above, when $s = 4$ we obtain $g(WBF(2, D)) \geqslant 2.0218\log(n) - o(\log(n))$ and $g(DB(2, D)) \geqslant 1.8133\log(n) - o(\log(n))$. We believe that using our methods better lower bounds can be obtained also for other networks.

Our lower bound technique is general and not limited to systolic protocols, since for $s \to \infty$ as a simple corollary it allows the determination of improved lower bounds even in the unrestricted (non-systolic) cases.

In fact, for general networks and $s \to \infty$, $\lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)} \approx \lambda + \lambda^3 + \cdots + \lambda^{s-1} = \lambda/(1-\lambda^2) = 1$ if $1/\lambda$ is equal to the golden ratio, thus yielding a lower bound of $1.4404\log(n) - O(\log\log(n))$ holding for all graphs and any (non-systolic) half-duplex gossip protocol. This result is only an $O(\log\log(n))$ additive factor far from the general one provided in [4,17,15,26].

More important, for specific networks it significantly improves with respect to the previously known directed and half-duplex lower bounds. As an example, for Wrapped Butterflies $g(WBF(2, D)) \geqslant 1.9750\log(n) - o(\log(n))$, while for de Bruijn networks $g(DB(2, D)) \geqslant 1.5876\log(n) - o(\log(n))$. Moreover, even more significant improvements can be obtained for less investigated topologies, such as Unwrapped Butterflies, directed Wrapped Butterflies, and Kautz networks. A more complete list of the related results can be found in Fig. 6. Similar considerations hold also for non-systolic full-duplex protocols (see Fig. 8).

The paper is organized as follows. In the next section we give some useful definitions and properties on matrices and norms. In Section 3, we introduce the notation and necessary definitions. In Section 4, we provide the general lower bound on the gossiping time in the directed and half-duplex cases. In Section 5, we generalize our technique to deal with specific topologies and we give lower bounds for Butterfly, de Bruijn and Kautz networks in the directed and half-duplex cases. In Section 6, we extend all the results to the full-duplex case and finally, in Section 7, we give some conclusive remarks.

## 2. Matrices and norms

We first introduce some useful definitions and properties about matrices. Except for some proved facts, all the properties below are well-known in linear algebra (see for instance [1]).

Let $\mathbb{R}^m$ be the set of all column vectors $\vec{x} = (x_1, \ldots, x_m)^T$ of $m$ real elements. A real function $|\,| : \mathbb{R}^m \to \mathbb{R}$ is called a *norm* if $|\vec{x}| \geqslant 0$ for every $\vec{x} \in \mathbb{R}^m$, $|\vec{x}| = 0$ if and only if all the $m$ components of $\vec{x}$ are equal to 0, $|a\vec{x}| = abs(a)|\vec{x}|$ for every $a \in \mathbb{R}$ and $\vec{x} \in \mathbb{R}^m$ ($abs(a)$ being the absolute value of

$a$), and finally $|\vec{X}+\vec{Y}| \leqslant |\vec{X}|+|\vec{Y}|$ for all $\vec{X},\vec{Y} \in \mathbb{R}^m$. The natural matrix norm of an $n \times m$ real matrix $M$ associated with a vector norm $|\vec{X}|$ is defined as $||M|| = \sup_{\vec{X}\in\mathbb{R}^m,|\vec{X}|\neq 0} \frac{|M\vec{X}|}{|\vec{X}|}$.

The Euclidean norm of a vector $\vec{X} \in \mathbb{R}^m$ is defined as $|\vec{X}|_2 = \sqrt{x_1^2+\cdots+x_m^2}$. The Euclidean matrix norm $||M||_2$ of an $n \times m$ real matrix $M$ is the natural matrix norm associated with $|\vec{X}|_2$. For the sake of brevity, in the sequel we will denote $|\ |_2$ and $||\ ||_2$ simply as $|\ |$ and $||\ ||$, respectively.

For every matrix $M$ with non negative real elements, the Euclidean matrix norm satisfies the following properties:

1. $||M|| \geqslant 0$;
2. $||M|| = 0 \Rightarrow M = 0$;
3. $\forall a \in \mathbb{R}$, $||aM|| = abs(a)||M||$;
4. $M \geqslant N$ (i.e., $M_{i,j} \geqslant N_{i,j}\ \forall i,j$) $\Rightarrow ||M|| \geqslant ||N||$;
5. $||M+N|| \leqslant ||M|| + ||N||$;
6. $||MN|| \leqslant ||M|| \cdot ||N||$;
7. if $N$ is obtained from $M$ by row and column permutations, $||N|| = ||M||$;
8. if $M$ is everywhere null except in $k$ subblocks $M_1,\ldots,M_k$ not sharing any row or column, then $||M|| = max_{i=1}^{k}||M_i||$.

**Definition 2.1.** Given an $m \times m$ real matrix $M$, a non null column vector $\vec{X} \in \mathbb{R}^m$ is an *eigenvector* for $M$ with *eigenvalue* $e$ if $M\vec{X} = e\vec{X}$. The spectral radius $\rho(M)$ of $M$ is the maximum absolute value of an eigenvalue of $M$.

The spectral radius of a matrix $M$ is related to the Euclidean norm of $M$. In fact, $||M|| = \sqrt{\rho(M^{\mathrm{T}}M)}$, where $M^{\mathrm{T}}$ is the transpose of $M$, and if $M$ is symmetric $||M|| = \rho(M)$. Moreover, for any natural matrix norm $||M||'$ associated with a vector norm $|\vec{X}|'$, $||M||' \geqslant \rho(M)$.

The following relaxation of eigenvectors and eigenvalues is non-standard and it is introduced only for the purposes of this paper.

**Definition 2.2.** Given an $m \times m$ matrix $M$, a non null column vector $\vec{X} \in \mathbb{R}^m$ is a *semi-eigenvector* for $M$ with *semi-eigenvalue* $e$ if $M\vec{X} \leqslant e\vec{X}$.

**Lemma 2.1.** *Given an $m \times m$ non negative matrix $M$ and a (strictly) positive semi-eigenvector $\vec{X} \in \mathbb{R}^m$ of $M$ with semi-eigenvalue $e$, $\rho(M) \leqslant e$.*

**Proof.** Let $\vec{X} = (x_1,\ldots,x_m)^{\mathrm{T}} \in \mathbb{R}^m$ be the semi-eigenvector and let $x_i > 0$ for each $i, 1 \leqslant i \leqslant m$. Then, given any $\vec{z} \in \mathbb{R}_m$, the function $|\vec{z}|_{\vec{X}} = \max_i \left(abs\left(\frac{z_i}{x_i}\right)\right)$ is a norm. In fact, it is easy to check that $|\vec{z}|_{\vec{X}} \geqslant 0$ for every $\vec{z} \in \mathbb{R}^m$, $|\vec{z}|_{\vec{X}} = 0$ if and only if all the $m$ components of $\vec{z}$ are equal to 0, $|a\vec{z}|_{\vec{X}} = abs(a)|\vec{z}|_{\vec{X}}$ for every $a \in \mathbb{R}$ and $\vec{z} \in \mathbb{R}^m$ and finally, since for every $i, 1 \leqslant i \leqslant m$, $abs(\frac{z_i+y_i}{x_i}) \leqslant abs(\frac{z_i}{x_i}) + abs(\frac{y_i}{x_i}) \leqslant |\vec{z}|_{\vec{X}} + |\vec{Y}|_{\vec{X}}$, $|\vec{z}+\vec{Y}|_{\vec{X}} \leqslant |\vec{z}|_{\vec{X}} + |\vec{Y}|_{\vec{X}}$ for all $\vec{z},\vec{Y} \in \mathbb{R}^m$.

Let $||\ ||_{\vec{X}}$ be the natural matrix norm associated with $|\ |_{\vec{X}}$.

Since $M$ is a non negative matrix, $||M||_{\vec{X}} = |M\vec{X}|_{\vec{X}}$. In fact, $||M||_{\vec{X}} \geqslant \frac{|M\vec{X}|_{\vec{X}}}{|\vec{X}|_{\vec{X}}} = |M\vec{X}|_{\vec{X}}$ and, for any vector $\vec{z}$, the vector $\vec{Y}$ with $y_i = |\vec{z}|_{\vec{X}} x_i$ is such that $|\vec{Y}|_{\vec{X}} = |\vec{z}|_{\vec{X}}$ and for every $i, 1 \leqslant i \leqslant m$, $y_i \geqslant z_i$; therefore $\frac{|M\vec{z}|_{\vec{X}}}{|\vec{z}|_{\vec{X}}} \leqslant \frac{|M\vec{Y}|_{\vec{X}}}{|\vec{Y}|_{\vec{X}}} = |M\vec{X}|_{\vec{X}}$.

Since $\vec{x}$ is a positive semi-eigenvector of $M$ and $M$ is non-negative, the corresponding semi-eigenvalue $e$ cannot be negative. Then, $e = e|\vec{x}|_{\vec{x}} \geqslant |M\vec{x}|_{\vec{x}} = ||M||_{\vec{x}} \geqslant \rho(M)$ (the latter inequality being verified for every natural matrix norm). □

Given two vector spaces $\mathcal{U}$ and $\mathcal{V}$, respectively of dimension $m$ and $n$, let the $m$ vectors $\vec{x}_1, \ldots, \vec{x}_m \in \mathcal{U}$ be a base for $\mathcal{U}$ and the $n$ vectors $\vec{y}_1, \ldots, \vec{y}_n \in \mathcal{V}$ be a base for $\mathcal{V}$. For any vector $\vec{x} \in \mathcal{U}$ let $\vec{x}_{\mathcal{U}} = (a_1, \ldots, a_m)^{\mathrm{T}}$ be the column vector that expresses $\vec{x}$ in terms of the base $\vec{x}_1, \ldots, \vec{x}_m$ of $\mathcal{U}$, i.e., such that $\vec{x} = \sum_{i=1}^{n} a_i \vec{x}_i$, and for any $\vec{y} \in \mathcal{V}$ let $\vec{y}_{\mathcal{V}}$ be similarly defined.

A function $f : \mathcal{U} \to \mathcal{V}$ is called a *linear mapping* if for every two vectors $\vec{x}, \vec{y} \in \mathcal{U}$ and for every two real numbers $a, b \in \mathbb{R}$, $f(a\vec{x} + b\vec{y}) = af(\vec{x}) + bf(\vec{y})$.

The linear mapping $f$ is completely specified by the image of the vectors $\vec{x}_1, \ldots, \vec{x}_m$, expressed in terms of $\vec{y}_1, \ldots, \vec{y}_n$. Then, in a natural way it is possible to associate with $f$ an $n \times m$ real matrix $M$ in which column $j$ is equal to $f(\vec{x}_j)_{\mathcal{V}}$, that is $f(\vec{x}_j) = \sum_{i=1}^{n} M_{i,j}\vec{y}_i$. Such a matrix satisfies the property that $M\vec{z}_{\mathcal{U}} = f(\vec{z})_{\mathcal{V}}$ for any vector $\vec{z} \in \mathcal{U}$.

Vice versa, for fixed bases of $\mathcal{U}$ and $\mathcal{V}$, each $n \times m$ matrix $M$ corresponds to a linear mapping from $\mathcal{U}$ to $\mathcal{V}$.

Let $\vec{x}'_1, \ldots, \vec{x}'_{m'}$ be $m' \leqslant m$ linearly independent vectors in $\mathcal{U}$, and let $P$ be the matrix in which column $j$ is equal to $\vec{x}'_{j\mathcal{U}}$, $1 \leqslant j \leqslant m'$, that is $\vec{x}'_j$ expressed in the base of $\mathcal{U}$. Moreover, let $\mathcal{U}' \subseteq \mathcal{U}$ be the subspace of $\mathcal{U}$ generated by $\vec{x}'_1, \ldots, \vec{x}'_{m'}$. Then $MP$ is the matrix associated to the restriction $f' : \mathcal{U}' \to \mathcal{V}$ of the linear mapping f to $\mathcal{U}'$, where $\vec{x}'_1, \ldots, \vec{x}'_{m'}$ is the base associated $\mathcal{U}'$ and $\vec{y}_1, \ldots, \vec{y}_n$ is still the base of $\mathcal{V}$. In fact, column $j$ of $MP$ corresponds to $f(\vec{x}'_j)_{\mathcal{V}}$, as it is equal to $M\vec{x}'_{j\mathcal{U}}$.

Given three vector spaces $\mathcal{U}, V, W$ with their respective bases and two linear mappings $f : \mathcal{U} \to \mathcal{V}$ and $g : \mathcal{V} \to \mathcal{W}$, let $M$ and $N$ be the matrices corresponding to $f$ and $g$ in the fixed bases, respectively. Then, the product $NM$ is the matrix associated with the linear mapping $(g \circ f) : \mathcal{U} \to \mathcal{W}$ resulting from the composition of $g$ and $f$ (i.e., $(g \circ f)(\vec{x}) = g(f(\vec{x}))$), still in the corresponding bases.

We now turn our attention to the case in which $\mathcal{U} = \mathcal{V}$. Let the $m \times m$ matrix $M$ be the matrix associated with $f$ in a given base (the same base is used to express the arguments and the values of $f$), and let $f(\mathcal{U}) \subseteq \mathcal{U}$ be the vector subspace constituted by all vectors $\vec{y} \in \mathcal{U}$ that are in the image of $f$, that is $f(\mathcal{U}) = \{f(\vec{x}) \mid \vec{x} \in \mathcal{U}\}$. Let us consider the matrix $M'$ associated with the restriction $f' : f(\mathcal{U}) \to f(\mathcal{U})$ of $f$ to $f(\mathcal{U})$, expressed in terms of another given base for $f(\mathcal{U})$. Then it is possible to prove the following lemma.

**Lemma 2.2.** $\rho(M) = \rho(M')$.

**Proof.** It is sufficient to show that the matrix $M'$ associated with $f'$ has the same eigenvalues as the matrix $M$ associated with $f$.

Let $\vec{x}_1, \ldots, \vec{x}_m$ be the base of $\mathcal{U}$ and let $\vec{x}'_1, \ldots, \vec{x}'_k$ the base of $f(\mathcal{U})$. Observe first that each eigenvector of $M$ belongs to $f(\mathcal{U})$. In fact, let $\vec{x} \in \mathcal{U}$ be such that $\vec{x}_{\mathcal{U}}$ is an eigenvector of $M$, that is it satisfies the equality $M\vec{x}_{\mathcal{U}} = e\vec{x}_{\mathcal{U}}$ for an eigenvalue $e$. Then $f(\vec{x}) = e\vec{x}$ (as the starting and final bases of $M$ coincide) and, since $f(\vec{x}/e) = \vec{x}$, $\vec{x} \in f(\mathcal{U})$.

To prove the claim, it is then sufficient to observe that $M\vec{x}_{\mathcal{U}} = e\vec{x}_{\mathcal{U}}$ if and only if $f(\vec{x}) = e\vec{x}$ if and only if $f'(\vec{x}) = e\vec{x}$ if and only if $M'\vec{x}_{f(\mathcal{U})} = e\vec{x}_{f(\mathcal{U})}$, and thus $e$ is an eigenvalue of $M$ if and only if it is an eigenvalue of $M'$. □

## 3. Preliminaries

We model the network as a digraph $G = (V, A)$ in which vertices represent processors and arcs communication links. Given an arc $(u, v) \in A$, $u$ and $v$ are called the endpoints of $(u, v)$.

**Definition 3.1.** A gossip protocol of length $t$ *for* $G = (V, A)$ *is a sequence* $\langle A_1, \ldots, A_t \rangle$ *of* $t$ *subsets* $A_1, \ldots, A_t \subseteq A$ *subject to the following conditions:*

1. *each* $A_i$, $1 \leqslant i \leqslant t$, *is a matching in* $G$ *(i.e., no two arcs in* $A_i$ *have a common endpoint),*
2. *for each two vertices* $x, y \in V$, *there exists a path* $P = \langle x_0, x_1, \ldots, x_l \rangle$ *with* $l \leqslant t$, $x_0 = x$ *and* $x_l = y$, *and a sequence of positive integers* $j_1, \ldots, j_l$ *such that* $1 \leqslant j_1 < \ldots < j_l \leqslant t$ *and for every* $i$, $1 \leqslant i \leqslant l$, $(x_{i-1}, x_i)$ *belongs to* $A_{j_i}$.

Informally, each $A_i$ represents the set of the arcs which are active at the communication round $i$. If an arc $(x, y)$ is active at a step $i$, then at the beginning of step $i + 1$ vertex $y$ additionally knows all the items known by $x$ at the beginning of step $i$. Then, in order for the sequence of the subsets $A_i$ to be a gossip procedure, for any two vertices $x$ and $y$ there must exist a directed path from $x$ to $y$ whose arcs are activated in a proper sequence so that at the end of the protocol $y$ knows the item of $x$.

If we restrict our attention to symmetric digraphs, then the above definition corresponds to half-duplex gossip protocols. To obtain the full-duplex case, it is sufficient to slightly modify the condition on the active arcs by saying that at every communication round if $(x, y)$ is active then also $(y, x)$ is active, i.e., any two active arcs either do not have a common endpoint or are opposite.

**Definition 3.2** ([8])**.** A gossip protocol $\langle A_1, \ldots, A_t \rangle$ for $G = (V, A)$ is $s$-systolic if for any $i, 1 \leqslant i \leqslant t - s$, $A_i = A_{i+s}$.

To prove the lower bounds, we now introduce the notion of *delay digraph* of a systolic gossip protocol.

**Definition 3.3.** The delay digraph $DG(A_1, \ldots, A_t)$, or simply $DG$, of an $s$-systolic gossip protocol $\langle A_1, \ldots, A_t \rangle$ for $G$ is a weighted digraph $DG = (V', A')$ with $V' = \{(x, y, i) \mid (x, y) \in A_i\}$, $A' = \{((x, y, i), (y, z, j)) \mid (x, y, i) \in V', (y, z, j) \in V', 1 \leqslant j - i < s\}$ and weight function $\delta((x, y, i), (y, z, j)) = j - i$.

In $DG$ each $(x, y, i) \in V'$ represents the activation of an arc $(x, y)$ during round $i$ and if there is an arc between $(x, y, i) \in V'$ and $(y, z, j) \in V'$ in $DG$, then $\delta((x, y, i), (y, z, j)) = j - i$ is the delay encountered by an item passing $(x, y)$ at time $i$ to cross $(y, z)$ at time $j$. Notice that, since the protocol is $s$-systolic, it is sufficient to represent in $DG$ only the delays within the next $s - 1$ rounds (i.e., for $j - i < s$), as the successive ones will correspond to the same activated edges.

Generalizing the above argument, if $(x, y, i) \in V'$ and $(w, z, j) \in V'$ are such that $(x, y, i) \neq (w, z, j)$ and their distance in $DG$ is at most $l$, then $j - i \leqslant l$ is the overall delay between $(x, y, i)$ and $(w, z, j)$, i.e., an item traversing $(x, y)$ during round $i$ steps through arc $(w, z)$ after at most $l$ rounds.

**Definition 3.4.** Given an $s$-systolic gossip protocol $\langle A_1, \ldots, A_t \rangle$ for $G$ with delay digraph $DG$ and a strictly positive real number $\lambda < 1$, the *delay matrix* $M^{DG}(\lambda)$, or simply $M(\lambda)$, of $G$ with respect to the $s$-systolic gossip protocol is the $|V'| \times |V'|$ matrix such that $M(\lambda)_{(x,y,i),(y,z,j)} = \lambda^{\delta((x,y,i),(y,z,j))}$ if $((x,y,i),(y,z,j)) \in A'$, else $M(\lambda)_{(x,y,i),(y,z,j)} = 0$.

The key property of the matrix $M(\lambda)$ is that, for any positive integer $t$, $(M(\lambda))^t_{(x,y,i),(w,z,j)} = \sum_{i=1}^{m} \lambda^{l_i}$, where $m$ is the number of dipaths of $t$ arcs from $(x,y,i)$ to $(w,z,j)$ in $DG$ and $l_1, \ldots, l_m$ their respective lengths, i.e., the sum of their arc weights. Then, if $(x,y,i) \neq (w,z,j)$ and there exists a dipath of length at most $l$ from $(x,y,i)$ to $(w,z,j)$ having no more than $t$ arcs, as $0 < \lambda < 1$ it is $\sum_{i=1}^{t} (M(\lambda))^i_{(x,y,i),(w,z,j)} \geqslant \lambda^l$.

Before proceeding with the determination of the general lower bound in the half-duplex mode, in the remaining part of this section we introduce some definitions and preliminary results related to specific interconnection networks. In fact, as we will see in the sequel, better lower bounds can be obtained if more information about the topology is known. In particular, this is possible for classes or families of networks containing a large number of faraway vertices.

**Definition 3.5.** Given a family $\mathcal{G}$ of arbitrarily large digraphs and two positive real numbers $\alpha$ and $l$, $\mathcal{G}$ has an $\langle \alpha, l \rangle$-separator if, for every digraph $G = (V,A) \in \mathcal{G}$, there exist two subsets of vertices $V_1 \subset V$ and $V_2 \subset V$ such that $min_{x \in V_1, y \in V_2} dist_G(x,y) = l \log(n) - o(\log(n))$ and $min(|V_1|, |V_2|) \geqslant 2^{\alpha l \log(n) - O(\log(n))}$, where $n = |V|$.

Notice that in the above definition $\alpha$ and $l$ depend on the family $\mathcal{G}$ and not on the single digraphs in $\mathcal{G}$. In particular, for every $G \in \mathcal{G}$, $\alpha$, and $l$ are not a function of the number of vertices of $G$. Moreover, by definition the inequality $\alpha \cdot l \leqslant 1$ always holds.

In the following, when dealing with digraphs $G$ whose corresponding families $\mathcal{G}$ are clear from the context, for the sake of brevity we will often identify $\mathcal{G}$ simply by $G$. So for instance we will say that $G$ has an $\langle \alpha, l \rangle$-separator to mean that $\mathcal{G}$ has such a separator.

The networks considered in this paper for the determination of the topology dependent lower bounds are all related to the standard hypercube in the sense that they maintain its basic properties while reducing the vertex degree from logarithmic to constant and maintaining a logarithmic diameter. In particular, they allow an efficient routing, the efficient simulation of arbitrary bounded degree networks and the fast implementation of algorithms like sorting and FFT (see [19]).

A *Butterfly digraph* of degree $d$ and dimension $D$, denoted by $BF(d,D)$, has as vertices the $(D+1)d^D$ tuples $(x,l) \in \{1, \ldots, d\}^D \times \{0, \ldots, D\}$, where $x = x_{D-1}x_{D-2} \ldots x_1x_0$ is a string of length $D$ over $\{1, \ldots, d\}$ and $l \in \{0, \ldots, D\}$ is an integer called level. A vertex $(x_{D-1}x_{D-2} \ldots x_1x_0, l)$ with $l > 0$ is joined with pairwise opposite arcs to the $d$ vertices $(x_{D-1} \ldots x_l, \alpha, x_{l-2}, \ldots x_0, l-1)$ such that $\alpha \in \{1, \ldots, d\}$.

A *Wrapped Butterfly digraph* of degree $d$ and dimension $D$, denoted by $\vec{WBF}(d,D)$, has as vertices the $Dd^D$ tuples $(x,l) \in \{1, \ldots, d\}^D \times \{0, \ldots, D-1\}$, where $x = x_{D-1}x_{D-2} \ldots x_1x_0$ is a string of length $D$ over $\{1, \ldots, d\}$ and $l \in \{0, \ldots, D-1\}$ is an integer called level. A vertex $(x_{D-1}x_{D-2} \ldots x_1x_0, l)$ with $l > 0$ has an arc toward the $d$ vertices $(x_{D-1} \ldots x_l \alpha x_{l-2} \ldots x_0, l-1)$ such that $\alpha \in \{1, \ldots, d\}$ and each vertex $(x_{D-1}x_{D-2} \ldots x_1x_0, 0)$ has an arc toward the $d$ vertices $(\alpha x_{D-2} \ldots x_1x_0, D-1)$ with $\alpha \in \{1, \ldots, d\}$. The corresponding undirected graph obtained by add-

ing the opposite of each arc is denoted as $WBF(d,D)$ and is generally called Wrapped Butterfly graph.

A *de Bruijn digraph* of degree $d$ and dimension $D$, denoted by $\vec{DB}(d,D)$, has as vertices all the $d^D$ strings of length $D$ over $\{1,\ldots,d\}$. Any vertex $x_{D-1}x_{D-2}\ldots x_1x_0$ has an arc toward the $d$ vertices $x_{D-2}x_{D-3}\ldots x_1x_0\alpha$ such that $\alpha\in\{1,\ldots,d\}$. The corresponding undirected graph, denoted as $DB(d,D)$, is called de Bruijn graph.

A *Kautz digraph* of degree $d$ and dimension $D$, denoted by $\vec{K}(d,D)$, has as vertices all the $(d+1)d^{D-1}$ strings $x_{D-1}x_{D-2}\ldots x_1x_0$ of length $D$ over $\{1,\ldots,d+1\}$ such that for any $j$, $0\leqslant j\leqslant D-2$, $x_j\neq x_{j+1}$. Any vertex $x_{D-1}x_{D-2}\ldots x_1x_0$ has an arc toward the $d$ vertices $x_{D-2}x_{D-3}\ldots x_1x_0\alpha$ with $\alpha\in\{1,\ldots,d+1\}$ and $\alpha\neq x_0$. The corresponding undirected graph, denoted as $K(d,D)$, is called Kautz graph.

The families of the Butterfly, de Bruijn, and Kautz networks with fixed degree $d$ have good separators.

**Lemma 3.1.** *There exists an $\langle\alpha,l\rangle$-separator with*

1. $\alpha=\log(d)/2$ *and* $l=2/\log(d)$ *for* $BF(d,D)$;
2. $\alpha=\log(d)/2$ *and* $l=2/\log(d)$ *for* $\vec{WBF}(d,D)$;
3. $\alpha=2\log(d)/3$ *and* $l=3/(2\log(d))$ *for* $WBF(d,D)$;
4. $\alpha=\log(d)$ *and* $l=1/\log(d)$ *for* $DB(d,D)$;
5. $\alpha=\log(d)$ *and* $l=1/\log(d)$ *for* $K(d,D)$.

**Proof.** For $BF(d,D)$ let $V_1=\{(x_{D-1}x_{D-2}\ldots x_1x_0,l)\mid x_{D-1}\leqslant\lfloor d/2\rfloor$ *and* $l=0\}$ and $V_2=\{(x_{D-1}x_{D-2}\ldots x_1x_0,l)\mid x_{D-1}>\lfloor d/2\rfloor$ *and* $l=0\}$. Since $n=(D+1)d^D$, $dist(V_1,V_2)=2D=2\log_d(n)-\mathrm{O}(\log\log(n))=2\log(n)/\log(d)-\mathrm{o}(\log(n))$ and $min(|V_1|,|V_2|)\geqslant\lfloor d^D/2\rfloor\geqslant 2^{\log(n)-\mathrm{O}(\log(n))}$. Thus $V_1$ and $V_2$ yield an $\langle\alpha,l\rangle$-separator for $BF(d,D)$ with $\alpha=\log(d)/2$ and $l=2/\log(d)$.

For $\vec{WBF}(d,D)$ let $V_1=\{(x_{D-1}x_{D-2}\ldots x_1x_0,l)\mid x_{D-1}\leqslant\lfloor d/2\rfloor$ *and* $l=D-1\}$ and $V_2=\{(x_{D-1}x_{D-2}\ldots x_1x_0,l)\mid x_{D-1}>\lfloor d/2\rfloor$ *and* $l=0\}$. Then $dist(V_1,V_2)=2D-1=2\log_d(n)-\mathrm{O}(\log\log(n))=2\log(n)/\log(d)-\mathrm{o}(\log(n))$ and $min(|V_1|,|V_2|)\geqslant\lfloor d^D/2\rfloor\geqslant 2^{\log(n)-\mathrm{O}(\log(n))}$. Thus again $V_1$ and $V_2$ yield an $\langle\alpha,l\rangle$-separator for $\vec{WBF}(d,D)$ with $\alpha=\log(d)/2$ and $l=2/\log(d)$.

For $WBF(d,D)$ the separator is constructed as follows. Let $h=\lfloor\sqrt{D}\rfloor$ and $X_1=\{x_{D-1}x_{D-2}\ldots x_1x_0\in\{1,\ldots,d\}^D\mid x_{h\cdot j}\leqslant\lfloor d/2\rfloor,\ 0\leqslant j<\lfloor\sqrt{D}\rfloor\}$ and $X_2=\{x_{D-1}x_{D-2}\ldots x_1x_0\in\{1,\ldots,d\}^D\mid x_{h\cdot j}>\lfloor d/2\rfloor,\ 0\leqslant j<\lfloor\sqrt{D}\rfloor\}$. Thus all the strings in $X_1$ differ from all the strings in $X_2$ about every $\sqrt{D}$ positions. In order to get the claimed separator, let then $V_1=\{(x,l)\mid x\in X_1$ *and* $l=0\}$ and $V_2=\{(x,l)\mid x\in X_2$ *and* $l=\lfloor D/2\rfloor\}$. Then $dist(V_1,V_2)=3D/2-\mathrm{O}(\sqrt{D})=3\log_d(n)/2-\mathrm{O}(\sqrt{\log(n)})=3\log(n)/(2\log(d))-\mathrm{o}(\log(n))$ and $min(|V_1|,|V_2|)\geqslant d^{D-\sqrt{D}}\geqslant 2^{\log(n)-\mathrm{O}(\log(n))}$. Thus $V_1$ and $V_2$ yield an $\langle\alpha,l\rangle$-separator for $WBF(d,D)$ with $\alpha=2\log(d)/3$ and $l=3/(2\log(d))$.

For $DB(d,D)$ take $V_1=X_1$ and $V_2=X_2$, with $X_1$ and $X_2$ defined as above. Then $dist(V_1,V_2)=D-\mathrm{O}(\sqrt{D})=\log_d(n)-\mathrm{O}(\sqrt{\log(n)})=\log(n)/\log(d)-\mathrm{o}(\log(n))$ and $min(V_1,V_2)\geqslant d^{D-\sqrt{D}}\geqslant 2^{\log(n)-\mathrm{O}(\log(n))}$. Therefore $V_1$ and $V_2$ yield an $\langle\alpha,l\rangle$-separator for $DB(d,D)$ with $\alpha=\log(d)$ and $l=1/\log(d)$.

Finally, for $K(d,D)$ take $V_1=\{x_{D-1}x_{D-2}\ldots x_1x_0\in\{1,\ldots,d+1\}^D\mid x_i\neq x_{i+1},0\leqslant i\leqslant D-2$, and $x_{h\cdot j}\leqslant\lfloor d/2\rfloor,\ 0\leqslant j<\lfloor\sqrt{D}\rfloor\}$ and $V_2=\{x_{D-1}x_{D-2}\ldots x_1x_0\in\{1,\ldots,d+1\}^D\mid x_i\neq x_{i+1},0\leqslant i\leqslant D-2$, and $x_{h\cdot j}>\lfloor d/2\rfloor,\ 0\leqslant j\leqslant\lfloor\sqrt{D}\rfloor\}$. Then $dist(V_1,V_2)=D-\mathrm{O}(\sqrt{D})=\log_d(n)-\mathrm{O}(\sqrt{\log(n)})=$

$\log(n)/\log(d) - o(\log(n))$ and $min(V_1, V_2) \geqslant d^{D-\sqrt{D}} \geqslant 2^{\log(n)-O(\log(n))}$. Therefore $V_1$ and $V_2$ yield an $\langle \alpha, l \rangle$-separator for $K(d,D)$ with $\alpha = \log(d)$ and $l = 1/\log(d)$. □

## 4. A general lower bound

In this section, we provide a general lower bound on the gossiping time of the $s$-systolic gossip protocols which holds for any network in the directed and half-duplex cases. We will always implicitly assume $s > 2$, as for $s = 2$ the subgraph induced by $A_1 \cup A_2$ (i.e., the arcs activated in the first and in the second round) must trivially form a directed cycle along which items can traverse at most one arc per step, so that gossiping takes at least $n - 1$ rounds.

We now show the usefulness of the delay matrix $M(\lambda)$ of a protocol and of its norm.

**Theorem 4.1.** *Let $\langle A_1, \ldots, A_t \rangle$ be an $s$-systolic gossip protocol for a digraph $G = (V, A)$ and let $M(\lambda)$ be the delay matrix of $G$ with respect to $\langle A_1, \ldots, A_t \rangle$. Then $t > \frac{\log(n)}{\log(1/\lambda)} - \frac{2\log(t)}{\log(1/\lambda)}$, where $n = |V|$ and $\lambda$ is any real number such that $0 < \lambda < 1$ and $||M(\lambda)|| \leqslant 1$.*

**Proof.** Since the protocol has length $t$, for any pair of vertices $x \in V$ and $z \in V$, the item of $x$ reaches $z$ in at most $t$ rounds. Then, the path followed by the item will start with an arc $(x, y)$ outgoing from $x$ during a round $i \geqslant 1$ and will terminate with an arc $(w, z)$ incoming in $z$ during a round $j \leqslant t$. Thus, the two vertices $(x, y, i) \in V'$ and $(w, z, j) \in V'$ in the delay digraph $DG = (V', A')$ have distance at most $t$. Since all weights in $DG$ are at least equal to 1, any dipath in $DG$ from $(x, y, i)$ to $(w, z, j)$ of length at most $t$ is constituted by at most $t$ arcs. Therefore, by the properties of $M(\lambda)$, since $0 < \lambda < 1$

$$M(\lambda)_{(x,y,i),(w,z,j)} + (M(\lambda)^2)_{(x,y,i),(w,z,j)} + \cdots + (M(\lambda)^t)_{(x,y,i),(w,z,j)} \geqslant \lambda^t.$$

Let us fix for any two vertices $x \in V$ and $z \in V$ of $G$ with $x \neq z$ exactly one pair of vertices $(x, y, i) \in V'$ and $(w, z, j) \in V'$ with distance at most $t$ in $DG$ (clearly, there can be more than one pair). Let $m = |V'| \leqslant tn/2$ (every vertex in $G$ can have at most $t$ activated incident arcs, one per round) and let $N$ be the $m \times m$ boolean matrix $N$ such that, for every $x \in V$ and $z \in V$ with $x \neq z$, the element of $N$ in the row of $(x, y, i)$ and column of $(w, z, j)$ is equal to 1, while all the other elements are equal to 0. Then, by extending the above argument for a single source–destination pair to all possible pairs

$$M(\lambda) + M(\lambda)^2 + \cdots + M(\lambda)^t \geqslant \lambda^t N.$$

By the norm properties

$$||M(\lambda) + M(\lambda)^2 + \cdots + M(\lambda)^t|| \geqslant ||\lambda^t N|| = \lambda^t ||N||.$$

Moreover, if we denote by $\vec{1}$ the unit column vector of $m$ elements equal to 1 and by $a_i$ the number of elements equal to 1 in the $i$th row of $N$, then

$$||N|| = \sup_{\vec{X} \in \mathbb{R}^m} \frac{|N\vec{X}|}{|\vec{X}|} \geqslant \frac{|N\vec{1}|}{|\vec{1}|} = \frac{\sqrt{\sum_{i=1}^m a_i^2}}{\sqrt{m}} \geqslant \frac{\sum_{i=1}^m a_i}{m} \geqslant \frac{2(n-1)}{t},$$

since there are $n(n-1)$ entries equal to 1 in $N$, and at most $tn/2$ rows. Therefore

$$||M(\lambda)|| + ||M(\lambda)||^2 + \cdots + ||M(\lambda)||^t \geqslant ||M(\lambda)|| + ||M(\lambda)^2|| + \cdots + ||M(\lambda)^t|| \geqslant ||M(\lambda) + M(\lambda)^2 + \cdots + M(\lambda)^t|| \geqslant \lambda^t 2(n-1)/t.$$

As $||M(\lambda)|| \leqslant 1$

$$t \geqslant ||M(\lambda)|| + ||M(\lambda)||^2 + \cdots + ||M(\lambda)||^t \geqslant \lambda^t 2(n-1)/t,$$

that is $t \geqslant \frac{\log(n-1)-\log(t)-\log(t)+1}{\log(1/\lambda)} > \frac{\log(n)}{\log(1/\lambda)} - \frac{2\log(t)}{\log(1/\lambda)}$. □

As a direct consequence of Theorem 4.1, the problem of deriving lower bounds on the gossiping time is reduced to the determination of the norm of the matrix $M(\lambda)$ associated with the $s$-systolic gossip protocol. We now show how this can be accomplished by means of successive simplification steps performed on $M(\lambda)$.

Observe first that, by the properties of the matrix norm, the value of $||M(\lambda)||$ is not affected by any row or column permutation of $M(\lambda)$. By the definition of $DG$, for every vertex $x$ of the initial graph $G$, all vertices $(y,x,i)$ in $DG$ can be connected only to vertices $(x,z,j)$ in $DG$ and to no other vertex of $DG$. It is then possible to permute the rows of $M(\lambda)$ in such a way that for every $x$ all vertices $(y,x,i)$ in $DG$ correspond to adjacent rows and all vertices $(x,z,j)$ to adjacent columns. The resulting matrix is everywhere null, except in $n$ disjoint subblocks not sharing any row or column. Informally, each subblock $M_x(\lambda)$ in $M(\lambda)$ corresponds to a vertex $x$ of the initial graph $G$ and reports the delays between its incoming and its outgoing arcs.

By the properties of the matrix norm $||M(\lambda)|| = max_x||M_x(\lambda)||$, hence in the remaining part of this section we concentrate on the determination of each $||M_x(\lambda)||$.

As already observed, $M_x(\lambda)$ expresses the local protocol occurring around a fixed vertex $x$ in $G$. Every row of $M_x(\lambda)$ corresponds to a *left activation* of $x$, that is to a vertex $(y,x,i)$ in the delay graph $DG$. In other words, a left activation is associated with the activation of an incoming arc of $x$. Analogously, every column corresponds to a *right activation* of $x$, that is to a vertex $(x,y,j)$ of $DG$.

We implicitly assume that at each round an arc incident to $x$ is activated. In fact, any local matrix not satisfying this property can be obtained from one in which the property is satisfied (which corresponds to a complete local protocol at vertex $x$) by deleting the rows corresponding to the removed left activations and the columns corresponding to the removed right activations. This cannot increase $||M_x(\lambda)||$ and, since in order to apply Theorem 4.1 we are interested in determining upper bounds for $||M_x(\lambda)||$, it does not affect the correctness of our proof.

To describe the properties of $M_x(\lambda)$, we first point out that an $s$-systolic protocol locally at the vertex $x$ is characterized by two sequences of positive integers $\langle (l_j)_{j=\{0,\cdots,k-1\}}, (r_j)_{j=\{0,\cdots,k-1\}} \rangle$. In fact, let $i$ be the first round such that there is a vertex $(y,x,i)$ in $DG$, i.e., such that there is a left activation at round $i$. Starting from round $i$, the protocol locally at $x$ has $l_0$ successive left activations (from round $i$ to round $i+l_0-1$), then $r_0$ successive right activations, then again $l_1$ left activations and $r_1$ right activations, and so on until the last $l_{k-1}$ left activations and $r_{k-1}$ right activations, where $k$ is a suitable positive integer such that $k \leqslant \lfloor s/2 \rfloor$. The last right activation corresponds to round $i+s-1$. Since the protocol is systolic, starting from round $i+s$ we have again $l_0$ left activations,

$r_0$ right activations and so forth, and this holds each $s$ rounds at times $i + j \cdot s$ with increasing $j$, till the end of the protocol. Clearly $\sum_{j=0}^{k-1}(l_j + r_j) = s$.

Consider now the last right activation of the whole protocol and assume that it corresponds to a particular $r_j, 0 \leqslant j \leqslant k-1$. Without loss of generality we can assume that the last right activation is complete, i.e., including $r_j$ right activations, as in a similar way as above $M_x(\lambda)$ can be obtained from a matrix satisfying this property by deleting some of the last columns and thus not increasing the matrix norm. Moreover, we may assume that the local protocol at $x$ starts with a left activation and ends with a right activation, since this corresponds to deleting initial columns of 0s and final rows of 0s in $M_x(\lambda)$, again without affecting its norm. We denote by $h$ the total number of left activation blocks (and thus right activation blocks) in $M_x(\lambda)$.

Since the protocol is $s$-systolic, it is possible to extend $\langle (l_j)_{j=\{0,\cdots,k-1\}}, (r_j)_{j=\{0,\cdots,k-1\}} \rangle$ to $\langle (l_j)_{j=\{0,\cdots,h-1\}}, (r_j)_{j=\{0,\cdots,h-1\}} \rangle$ in such a way that, for each $j \geqslant k$, $l_j = l_{j \bmod k}$ and $r_j = r_{j \bmod k}$.

**Definition 4.1.** *Given the couple of sequences* $\langle (l_j)_{j=\{0,\cdots,h-1\}}, (r_j)_{j=\{0,\cdots,h-1\}} \rangle$ *associated with the local protocol at vertex x, the left (resp. right)* activation block $j$ *is the set of the successive left (resp. right) activations corresponding to* $l_j$ *(resp.* $r_j$*).*

Hence for instance the left activation block 0 corresponds to the first $l_0$ left activations, block 1 to the next $l_1$ left activations, ..., block $k-1$ to the last $l_{k-1}$ activations within the period, and then again block $k$ to the next $l_k = l_0$ activations and so forth.

Since permuting rows and columns of $M_x(\lambda)$ does not affect $||M_x(\lambda)||$, we can assume the following ordering of the rows and columns of $M_x(\lambda)$:

- rows occur in order of left activation block and inside each block in reverse order of round. So for instance the first row corresponds to the $l_0$th left activation of block 0 and row $l_0$ to the first;
- columns occur in order of right activation block and inside each block this time in order of round. Hence column 1 is associated with the first right activation of block 0 and column $r_0$ to the last.

An example of $M_x(\lambda)$ can be found in Fig. 1 (with further details to be defined below).
The following vectors can be used to suitably express $M_x(\lambda)$:

- $\vec{0}^i$ is the null column vector of $i$ components;
- $\vec{\Lambda}^i = (1, \lambda, \ldots, \lambda^{i-1})^{\mathrm{T}}$;
- for ease of notation, given two column vectors $\vec{\mathrm{X}}$ and $\vec{\mathrm{Y}}$, respectively of $i$ and $j$ components, we denote as $\vec{\mathrm{X}}\vec{\mathrm{Y}} = (\vec{\mathrm{X}}^{\mathrm{T}}\vec{\mathrm{Y}}^{\mathrm{T}})^{\mathrm{T}}$ the *vertical concatenation* of $\vec{\mathrm{X}}$ and $\vec{\mathrm{Y}}$, i.e., the column vector of $i+j$ components such that the first $i$ components coincide with the ones of $\vec{\mathrm{X}}$ and the last remaining $j$ components coincide with the ones of $\vec{\mathrm{Y}}$.

By construction, $M_x(\lambda)$ can be divided in $h^2$ blocks $B_{0,0}, \ldots, B_{h-1,h-1}$ such that $B_{i,j}$ corresponds to the left activation block $i$ and the right activation block $j$ and is given by the intersection of the associated rows and columns (see Fig. 1). If $j < i$ or $j \geqslant i + k$ then $B_{i,j}$ has all entries equal to 0, since each left activation in block $i$ is related only to the right activations in the next $s-1$ rounds, i.e., in the right activation blocks from $i$ to $i + k - 1$. If $i \leqslant j < i + k$, then $B_{i,j}$ can be suitably expressed as

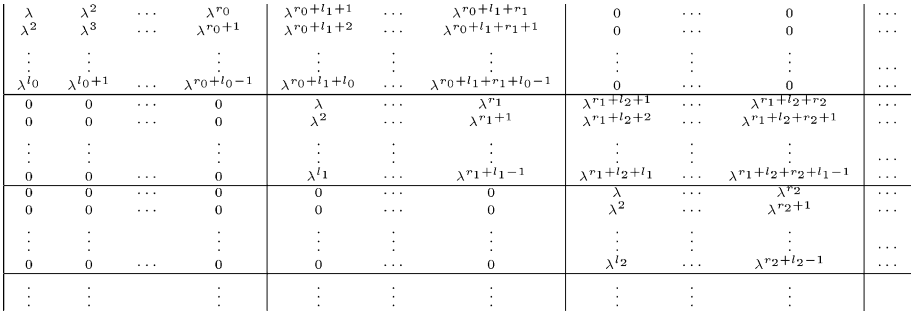

Fig. 1. $M_x(\lambda)$ for $k = 2$; we have emphasized blocks $B_{i,j}$ with $0 \leqslant i \leqslant 2$ and $0 \leqslant j \leqslant 2$.

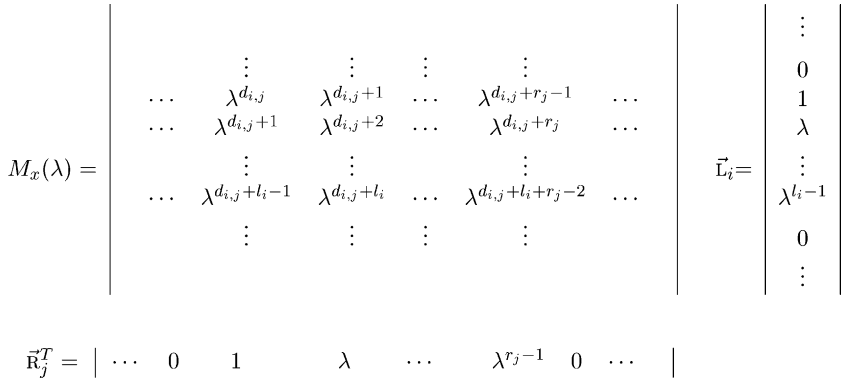

Fig. 2. Block $B_{i,j}$ in $M_x(\lambda)$ and vectors $\vec{\mathrm{L}}_i$ and $\vec{\mathrm{R}}_j^{\mathrm{T}}$.

$B_{i,j} = \lambda^{d_{i,j}} \vec{\Lambda}^{l_i} \left(\vec{\Lambda}^{r_j}\right)^{\mathrm{T}}$, where $d_{i,j}$ is the number of rounds between the last activation of the left activation block $i$ and the first activation of the right activation block $j$, that is $d_{i,j} = 1 + \sum_{c=i}^{j-1}(r_c + l_{c+1})$ (see Figs. 1 and 2).

$M_x(\lambda)$ has rank $h$. In fact, the $h$ orthogonal column vectors $\vec{\mathrm{L}}_0 = \vec{\Lambda}^{l_0}\vec{0}^{l_1} \ldots \vec{0}^{l_{h-1}}$, $\vec{\mathrm{L}}_1 = \vec{0}^{l_0}\vec{\Lambda}^{l_1}\vec{0}^{l_2} \ldots \vec{0}^{l_{h-1}}, \ldots, \vec{\mathrm{L}}_{h-1} = \vec{0}^{l_0} \ldots \vec{0}^{l_{h-2}}\vec{\Lambda}^{l_{h-1}}$ form a base for the vector space generated by the columns of $M_x(\lambda)$. Analogously, the column vectors $\vec{\mathrm{R}}_0 = \vec{\Lambda}^{r_0}\vec{0}^{r_1} \ldots \vec{0}^{r_{h-1}}$, $\vec{\mathrm{R}}_1 = \vec{0}^{r_0}\vec{\Lambda}^{r_1}\vec{0}^{r_2} \ldots \vec{0}^{r_{h-1}}, \ldots, \vec{\mathrm{R}}_{h-1} = \vec{0}^{r_0} \ldots \vec{0}^{r_{h-2}}\vec{\Lambda}^{r_{h-1}}$ form a base for the vector space generated by the transposition of the rows (again see Fig. 2).

Recalling the notation and definitions of Section 2, $M_x(\lambda)$ can be seen as the matrix associated with a linear mapping $f : \mathcal{U} \to \mathcal{V}$ from the vector space $\mathcal{U} = \mathbb{R}^{r_0+r_1+\cdots+r_{h-1}}$ to the vector space $\mathcal{V} = \mathbb{R}^{l_0+l_1+\cdots+l_{h-1}}$, where the arguments and values of $f$ are expressed in the natural bases $\vec{\mathrm{X}}_1, \ldots, \vec{\mathrm{X}}_{r_0+r_1+\cdots+r_{h-1}}$ and $\vec{\mathrm{Y}}_1, \ldots, \vec{\mathrm{Y}}_{l_0+l_1+\cdots+l_{h-1}}$, i.e., such that all the $r_0 + r_1 + \cdots + r_{h-1}$ components of each $\vec{\mathrm{X}}_i$, $1 \leqslant i \leqslant r_0 + r_1 + \cdots + r_{h-1}$, are equal to 0, except the $i$th one which is equal to 1, and similarly all the $l_0 + l_1 + \cdots + l_{h-1}$ components of each $\vec{\mathrm{Y}}_j$, $1 \leqslant j \leqslant l_0 + l_1 + \cdots + l_{h-1}$, are equal to 0, except the $j$th one which is equal to 1.

By the natural bases of $\mathcal{U}$, for each vector $\vec{\mathrm{X}} \in \mathcal{U}$, $\vec{\mathrm{X}} = \vec{\mathrm{X}}_{\mathcal{U}}$, that is $\vec{\mathrm{X}}$ coincides with the vector $\vec{\mathrm{X}}_{\mathcal{U}}$ that expresses $\vec{\mathrm{X}}$ in terms of the natural base of $\mathcal{U}$. Hence, in the following for the sake of brevity we denote $\vec{\mathrm{X}}_{\mathcal{U}}$ simply as $\vec{\mathrm{X}}$. Similarly, by the natural base of $\mathcal{V}$, for each $\vec{\mathrm{Y}} \in \mathcal{V}$, $\vec{\mathrm{Y}} = \vec{\mathrm{Y}}_{\mathcal{V}}$. In particular, this holds also for the vectors $\vec{\mathrm{R}}'_{i\mathcal{U}}$ and $\vec{\mathrm{L}}'_{j\mathcal{U}}$ that expressed in the respective natural bases are $\vec{\mathrm{R}}_i$ and $\vec{\mathrm{L}}_j$, $0 \leqslant i \leqslant h-1$ and $0 \leqslant j \leqslant h-1$.

Since all the columns of $M_x(\lambda)$ can be expressed as a linear combination of $\vec{\mathrm{L}}_0, \ldots, \vec{\mathrm{L}}_{h-1}$, then the subspace $f(\mathcal{U}) \subseteq \mathcal{V}$ of all the vectors that are in the image of $f$ has dimension $h$. If we want to determine the matrix $M'$ associated to $f : \mathcal{U} \to f(\mathcal{U})$ where the base of $f(\mathcal{U})$ is constituted by $\vec{\mathrm{L}}_0, \ldots, \vec{\mathrm{L}}_{h-1}$, then it suffices to consider the matrix $M'$ whose rows are in the order row 1, row $l_0 + 1$, ..., and row $l_{h-1} + 1$ of $M_x(\lambda)$. In fact, the $j$th column of $M'$ expresses $f(\vec{\mathrm{X}}_j)$ in terms of $\vec{\mathrm{L}}_0, \ldots, \vec{\mathrm{L}}_{h-1}$. More precisely, if the $j$th column of $M'$ is $(a_0, \ldots, a_{h-1})^{\mathrm{T}}$, then $\sum_{i=0}^{h-1} a_j \vec{\mathrm{L}}_j$ coincides with the $j$th column of $M_x(\lambda)$, that is to $f(\vec{\mathrm{X}}_j)$. Therefore, $f(\vec{\mathrm{X}}_j)_{f(\mathcal{U})} = (a_0, \ldots, a_{h-1})^{\mathrm{T}}$.

Moreover, as stated in Section 2, if we want to restrict $f$ on the subspace $\mathcal{U}' \subseteq \mathcal{U}$ generated by $h$ vectors $\vec{\mathrm{R}}_0, \ldots, \vec{\mathrm{R}}_{h-1}$, it suffices to multiply $M'$ with the matrix $P$ whose columns are $\vec{\mathrm{R}}_0, \ldots, \vec{\mathrm{R}}_{h-1}$, since for each $j$, $1 \leqslant j \leqslant k$, column $j$ is $M'\vec{\mathrm{R}}_j = f(\vec{\mathrm{R}}_j)_{f(\mathcal{U})}$, that is $f(\vec{\mathrm{R}}_j)$ expressed in terms of $\vec{\mathrm{L}}_0, \ldots, \vec{\mathrm{L}}_{h-1}$. Let us denote as $N_x(\lambda) = M'P$ the resulting matrix (see Fig. 3).

Summarizing the above argument, $N_x(\lambda)$ is the matrix associated with the linear mapping $f'$ which is the restriction of $f$ from the subspace of $\mathcal{U}' \subseteq \mathcal{U}$ generated by $\vec{\mathrm{R}}_0, \ldots, \vec{\mathrm{R}}_{h-1}$ to the subspace $f(\mathcal{U})$ generated by $\vec{\mathrm{L}}_0, \ldots, \vec{\mathrm{L}}_{h-1}$, where the bases of $\mathcal{U}'$ and $f(\mathcal{U})$ are $\vec{\mathrm{R}}_0, \ldots, \vec{\mathrm{R}}_{h-1}$ and $\vec{\mathrm{L}}_0, \ldots, \vec{\mathrm{L}}_{h-1}$, respectively.

By construction, the component of $N_x(\lambda)$ at row $i$ and column $j$ corresponds to block $B_{i,j}$ in $N_x(\lambda)$ and thus it is 0 if $j < i$ or $j \geqslant i + k$, otherwise $\lambda^{d_{i,j}} p_{r_j}(\lambda)$, where $d_{i,j}$ is defined like above as the number of rounds between the last activation of the left activation block $i$ and the next first activation of the right activation block $j$, while for any even positive integer $i$ the polynomial $p_i(\lambda) = 1 + \lambda^2 + \cdots + \lambda^{2i-2}$ (see Fig. 3).

A completely symmetric argument performed on the linear mapping $g : \mathcal{V} \to \mathcal{U}$ associated with the transpose matrix $M_x(\lambda)^{\mathrm{T}}$ allows to obtain a matrix $O_x(\lambda)$ associated with the linear mapping $g'$ which is the restriction of $g$ from the subspace of $\mathcal{V}' \subseteq \mathcal{V}$ generated by $\vec{\mathrm{L}}_0, \ldots, \vec{\mathrm{L}}_{h-1}$ to the subspace

$$N_x(\lambda) = \begin{vmatrix} \lambda p_{r_0}(\lambda) & \lambda^{r_0+l_1+1} p_{r_1}(\lambda) & 0 & 0 & \cdots \\ 0 & \lambda p_{r_1}(\lambda) & \lambda^{r_1+l_2+1} p_{r_2}(\lambda) & 0 & \cdots \\ 0 & 0 & \lambda p_{r_2}(\lambda) & \lambda^{r_2+l_3+1} p_{r_3}(\lambda) & \cdots \\ 0 & 0 & 0 & \lambda p_{r_3}(\lambda) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{vmatrix}$$

$$O_x(\lambda) = \begin{vmatrix} \lambda p_{l_0}(\lambda) & 0 & 0 & 0 & \cdots \\ \lambda^{r_0+l_1+1} p_{l_0}(\lambda) & \lambda p_{l_1}(\lambda) & 0 & 0 & \cdots \\ 0 & \lambda^{r_1+l_2+1} p_{l_1}(\lambda) & \lambda p_{l_2}(\lambda) & 0 & \cdots \\ 0 & 0 & \lambda^{r_2+l_3+1} p_{l_2}(\lambda) & \lambda p_{l_3}(\lambda) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{vmatrix}$$

Fig. 3. $N_x(\lambda)$ and $O_x(\lambda)$ for $k = 2$.

$g(\mathcal{V})$ generated by $\vec{\mathrm{R}}_0, \ldots, \vec{\mathrm{R}}_{h-1}$. The bases associated to $\mathcal{V}'$ and $g(\mathcal{V})$ are $\vec{\mathrm{L}}_0, \ldots, \vec{\mathrm{L}}_{h-1}$ and $\vec{\mathrm{R}}_0, \ldots, \vec{\mathrm{R}}_{h-1}$, respectively. In $O_x(\lambda)$ the component at row $i$ and column $j$ is 0 if $j \leqslant i-k$ or $j > i$, otherwise $\lambda^{d_{j,i}} p_{l_j}(\lambda)$ (again see Fig. 3).

Notice that $\mathcal{V}' = f(\mathcal{U})$ and $\mathcal{U}' = g(\mathcal{V})$. Moreover, since the vectors $f(\vec{\mathrm{R}}_0), \ldots, f(\vec{\mathrm{R}}_{h-1})$ generate $\mathcal{V}'$ (recall that by the natural base of $\mathcal{V}$ for each $i$, $0 \leqslant i \leqslant h-1$, $f(\vec{\mathrm{R}}_i) = M\vec{\mathrm{R}}_i$), $f(\mathcal{U}') = \mathcal{V}'$ and consequently $(g \circ f)(\mathcal{U}) = \mathcal{U}'$. Therefore $O_x(\lambda)N_x(\lambda)$, that is the matrix associated with the composition $g' \circ f'$, corresponds to the restriction of $g \circ f$ to $\mathcal{U}'$.

Let $\vec{\mathrm{E}} = (e_0, \ldots, e_{h-1})^{\mathrm{T}}$ be the column vector whose $j$th component $e_j = \lambda^{\sum_{c=0}^{j-1}(r_c - l_{c+1})}$, $1 \leqslant j \leqslant h-1$. Then, it is possible to prove the following lemma.

**Lemma 4.2.** *$\vec{\mathrm{E}}$ is a semi-eigenvector both of $N_x(\lambda)$ and $O_x(\lambda)$ with semi-eigenvalues $\lambda \cdot p_{r_0+\cdots+r_{k-1}}(\lambda)$ and $\lambda \cdot p_{l_0+\cdots+l_{k-1}}(\lambda)$, respectively.*

**Proof.** Let us show first that $\vec{\mathrm{E}}$ is a semi-eigenvector for $N_x(\lambda)$ with semi-eigenvalue $\lambda \cdot p_{r_0+\cdots+r_{k-1}}(\lambda)$.

Let $a_0, \ldots, a_{h-1}$ be the $h$ components of $N_x(\lambda)\vec{\mathrm{E}}$ and consider any $a_i$ with $0 \leqslant i \leqslant h-k$, i.e., such that $a_i$ is not one of the last $k-1$ components of $\vec{\mathrm{E}}$. Then

$$
\begin{aligned}
a_i &= \sum_{j=0}^{h-1} N_x(\lambda)_{i,j} \cdot e_j = \sum_{j=i}^{i+k-1} N_x(\lambda)_{i,j} \cdot e_j = \sum_{j=i}^{i+k-1} \lambda^{d_{i,j}} \cdot p_{r_j}(\lambda) \cdot e_j \\
&= \sum_{j=i}^{i+k-1} \lambda^{1+\sum_{c=i}^{j-1}(r_c + l_{c+1})} \cdot p_{r_j}(\lambda) \cdot \lambda^{\sum_{c=0}^{j-1}(r_c - l_{c+1})} \\
&= \lambda \cdot \lambda^{\sum_{c=0}^{i-1}(r_c - l_{c+1})} \sum_{j=i}^{i+k-1} \lambda^{\sum_{c=i}^{j-1}(r_c + l_{c+1})} \cdot p_{r_j}(\lambda) \cdot \lambda^{\sum_{c=i}^{j-1}(r_c - l_{c+1})} \\
&= \lambda \cdot \lambda^{\sum_{c=0}^{i-1}(r_c - l_{c+1})} \sum_{j=i}^{i+k-1} \lambda^{2\sum_{c=i}^{j-1} r_c} \cdot p_{r_j}(\lambda) \\
&= \lambda \cdot \lambda^{\sum_{c=0}^{i-1}(r_c - l_{c+1})} (p_{r_i}(\lambda) + \lambda^{2r_i} \cdot p_{r_{i+1}}(\lambda) + \lambda^{2(r_i + r_{i+1})} \cdot p_{r_{i+2}}(\lambda) + \cdots \\
&\quad + \lambda^{2(r_i + \cdots + r_{i+k-2})} \cdot p_{r_{i+k-1}}(\lambda)) = \lambda \cdot p_{r_i + r_{i+1} + \cdots + r_{i+k-1}}(\lambda) \cdot \lambda^{\sum_{c=0}^{i-1}(r_c - l_{c+1})} \\
&= \lambda \cdot p_{r_0 + r_1 + \cdots + r_{k-1}}(\lambda) \cdot e_i,
\end{aligned}
$$

since, as the protocol is $s$-systolic, $r_i + r_{i+1} + \cdots + r_{i+k-1} = r_0 + r_1 + \cdots + r_{k-1}$ and by definition of $p_i(\lambda)$ for any $j$ it results $p_i(\lambda) + \lambda^{2i} p_j(\lambda) = p_{i+j}(\lambda)$.

Concerning the last $k-1$ components of $N_x(\lambda)\vec{\mathrm{E}}$, the only difference is that each such component $a_i$ now is such that $a_i = \sum_{j=i}^{h-1} N_x(\lambda)_{i,j} \cdot e_j$ instead of $a_i = \sum_{j=i}^{i+k-1} N_x(\lambda)_{i,j} \cdot e_j$, i.e., the summation has less than $k$ terms. Thus, by the same considerations above, it results $a_i < \lambda \cdot p_{r_0 + r_1 + \cdots + r_{k-1}}(\lambda) \cdot e_i$ (this is actually the reason why we have semi-eigenvalues instead of eigenvalues).

It remains to show that $\vec{\mathrm{E}}$ is a semi-eigenvector for $O_x(\lambda)$ with semi-eigenvalue $\lambda \cdot p_{l_0+\cdots+l_{k-1}}(\lambda)$.

Let $b_0, \ldots, b_{h-1}$ be the $h$ components of $O_x(\lambda)\vec{\mathrm{E}}$ and consider any $b_i$ with $k-1 \leqslant i \leqslant h-1$, i.e., such that $b_i$ is not one of the first $k-1$ components of $\vec{\mathrm{E}}$. Then

$$
\begin{aligned}
b_i &= \sum_{j=0}^{h-1} O_x(\lambda)_{i,j} \cdot e_j = \sum_{j=i-k+1}^{i} O_x(\lambda)_{i,j} \cdot e_j = \sum_{j=i-k+1}^{i} \lambda^{d_{j,i}} \cdot p_{l_j}(\lambda) \cdot e_j \\
&= \sum_{j=i-k+1}^{i} \lambda^{1+\sum_{c=j}^{i-1}(r_c+l_{c+1})} \cdot p_{l_j}(\lambda) \cdot \lambda^{\sum_{c=0}^{j-1}(r_c-l_{c+1})} \\
&= \sum_{j=i-k+1}^{i} \lambda^{1+\sum_{c=j}^{i-1}(r_c+l_{c+1})} \cdot p_{l_j}(\lambda) \cdot \lambda^{\sum_{c=0}^{i-1}(r_c-l_{c+1})-\sum_{c=j}^{i-1}(r_c-l_{c+1})} \\
&= \lambda \cdot \lambda^{\sum_{c=0}^{i-1}(r_c-l_{c+1})} \sum_{j=i-k+1}^{i} p_{l_j}(\lambda) \cdot \lambda^{\sum_{c=j}^{i-1}(r_c+l_{c+1})-\sum_{c=j}^{i-1}(r_c-l_{c+1})} \\
&= \lambda \cdot \lambda^{\sum_{c=0}^{i-1}(r_c-l_{c+1})} \sum_{j=i-k+1}^{i} \lambda^{2\sum_{c=j}^{i-1} l_{c+1}} \cdot p_{l_j}(\lambda) \\
&= \lambda \cdot \lambda^{\sum_{c=0}^{i-1}(r_c-l_{c+1})} (p_{l_i}(\lambda) + \lambda^{2l_i} \cdot p_{l_{i-1}}(\lambda) + \lambda^{2(l_i+l_{i-1})} \cdot p_{l_{i-2}}(\lambda) + \cdots \\
&\quad + \lambda^{2(l_i+\cdots+l_{i-k+2})} \cdot p_{l_{i-k+1}}(\lambda)) = \lambda \cdot p_{l_i+l_{i-1}+\cdots+l_{i-k+1}}(\lambda) \cdot \lambda^{\sum_{c=0}^{i-1}(r_c-l_{c+1})} \\
&= \lambda \cdot p_{l_0+l_1+\cdots+l_{k-1}}(\lambda) \cdot e_i,
\end{aligned}
$$

since $l_i + l_{i-1} + \cdots + l_{i-k+1} = l_0 + l_1 + \cdots + l_{k-1}$.

Concerning the first $k-1$ components of $O_x(\lambda)\vec{\mathrm{E}}$, the only difference is that each such component $b_i$ now is such that $b_i = \sum_{j=0}^{i} O_x(\lambda)_{i,j} \cdot e_j$ instead of $b_i = \sum_{j=i-k+1}^{i} O_x(\lambda)_{i,j} \cdot e_j$, i.e., the summation has less than $k$ terms. Thus, by the same considerations above, it results $b_i < \lambda \cdot p_{l_0+l_1+\cdots+l_{k-1}}(\lambda) \cdot e_i$. □

We are now ready to prove an upper bound on the norm of $M(\lambda)$.

**Lemma 4.3.** $||M(\lambda)|| \leqslant \lambda\sqrt{p_{\lfloor s/2 \rfloor}(\lambda)}\sqrt{p_{\lceil s/2 \rceil}(\lambda)}$.

**Proof.** For any $x \in V$, let $f : \mathcal{U} \to \mathcal{V}$ (resp. $g : \mathcal{V} \to \mathcal{U}$) be the linear mapping associated with $M_x(\lambda)$ (resp. $M_x(\lambda)^{\mathrm{T}}$). Then $M_x(\lambda)^{\mathrm{T}} M_x(\lambda)$ corresponds to the composition $(g \circ f) : \mathcal{U} \to \mathcal{U}$ and $O_x(\lambda)N_x(\lambda)$ to the restriction of $g \circ f$ to the subspace $(g \circ f)(\mathcal{U}) \subseteq \mathcal{U}$ corresponding to the image of $g \circ f$ with base $\vec{\mathrm{R}}_0, \ldots, \vec{\mathrm{R}}_{h-1}$.

Since $(l_0 + \cdots + l_{k-1}) + (r_0 + \cdots + r_{k-1}) = s$, $p_{l_0+\cdots+l_{k-1}}(\lambda) \cdot p_{r_0+\cdots+r_{k-1}}(\lambda) \leqslant p_{\lfloor s/2 \rfloor}(\lambda) \cdot p_{\lceil s/2 \rceil}(\lambda)$. In fact, for $i \geqslant j$, $p_{i+1}(\lambda) \cdot p_{j-1}(\lambda) = p_{i+1}(\lambda) \cdot (p_j(\lambda) - \lambda^{2j-2}) = p_{i+1}(\lambda) \cdot p_j(\lambda) - \lambda^{2j-2} \cdot p_{i+1}(\lambda) = p_i(\lambda) \cdot p_j(\lambda) + \lambda^{2i} p_j(\lambda) - \lambda^{2j-2} \cdot p_{i+1}(\lambda) < p_i(\lambda) \cdot p_j(\lambda)$, as $\lambda^{2i} \cdot p_j(\lambda) - \lambda^{2j-2} \cdot p_{i+1}(\lambda) < 0$.

| period $s$ | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|
| $e(s)$ | 2.8808 | 1.8133 | 1.6502 | 1.5363 | 1.5021 | 1.4721 |

| period $s$ | 9 | 10 | 11 | 12 | ... | $\infty$ |
|---|---|---|---|---|---|---|
| $e(s)$ | 1.4617 | 1.4518 | 1.4481 | 1.4446 | ... | 1.4404 |

Fig. 4. General lower bound for different systolic periods in the directed and half-duplex cases. $t \geqslant e(s)\log(n) - O(\log\log(n))$. For limited $s$ no previous lower bounds known (except the ones inferred from broadcasting in [22,2]), while for $s = \infty$ the bound differs only $O(\log\log(n))$ from the one in [4,17,15,26].

By Lemma 4.2 $\vec{E}$ is a semi-eigenvector of $O_x(\lambda)N_x(\lambda)$ with semi-eigenvalue $\lambda^2 \cdot p_{l_0+\cdots+l_{k-1}}(\lambda) \cdot p_{r_0+\cdots+r_{k-1}}(\lambda)$, as $O_x(\lambda)N_x(\lambda)\vec{E} \leqslant O_x(\lambda)(\lambda \cdot p_{r_0+\cdots+r_{k-1}}(\lambda) \cdot \vec{E}) \leqslant \lambda^2 \cdot p_{l_0+\cdots+l_{k-1}}(\lambda) \cdot p_{r_0+\cdots+r_{k-1}}(\lambda) \cdot \vec{E} \leqslant \lambda^2 \cdot p_{\lfloor s/2\rfloor}(\lambda) \cdot p_{\lceil s/2\rceil}(\lambda) \cdot \vec{E}$.

By Lemma 2.1 $\rho(O_x(\lambda)N_x(\lambda)) \leqslant \lambda^2 \cdot p_{\lfloor s/2\rfloor}(\lambda) \cdot p_{\lceil s/2\rceil}(\lambda)$ and thus by applying Lemma 2.2 $||M_x(\lambda)|| = \sqrt{\rho\left(M_x(\lambda)^{\mathrm{T}}M_x(\lambda)\right)} = \sqrt{\rho(O_x(\lambda)N_x(\lambda))} \leqslant \lambda\sqrt{p_{\lfloor s/2\rfloor}(\lambda)}\sqrt{p_{\lceil s/2\rceil}(\lambda)}$. Therefore, $||M(\lambda)|| = max_x||M_x(\lambda)|| \leqslant \lambda\sqrt{p_{\lfloor s/2\rfloor}(\lambda)}\sqrt{p_{\lceil s/2\rceil}(\lambda)}$. □

From Theorem 4.1 and Lemma 4.3, the following corollary holds.

**Corollary 4.4.** *Let $\langle A_1, \ldots, A_t\rangle$ be an $s$-systolic gossip protocol for a digraph $G = (V, A)$. Then $t \geqslant e(s)\log(n) - O(\log\log(n))$, where $n = |V|, e(s) = \frac{1}{\log(1/\lambda)}$ and $\lambda$ is the unique real number such that $0 < \lambda < 1$ and $\lambda\sqrt{p_{\lfloor s/2\rfloor}(\lambda)}\sqrt{p_{\lceil s/2\rceil}(\lambda)} = 1$, with $p_i(\lambda) = 1 + \lambda^2 + \cdots + \lambda^{2i-2}$ for any integer $i > 0$.*

**Proof.** If $t \geqslant e(s)\log(n)$ the corollary trivially holds, otherwise it follows from Theorem 4.1 by observing that by Lemma 4.3 $||M(\lambda)|| \leqslant 1$ and, as $\lambda$ is independent of $n$, $\frac{2\log(t)}{\log(1/\lambda)} < \frac{2\log(e(s)\log(n))}{\log(1/\lambda)} = O(\log\log(n))$. □

Notice that, as it can be easily checked, $\lambda\sqrt{p_{\lfloor s/2\rfloor}(\lambda)}\sqrt{p_{\lceil s/2\rceil}(\lambda)}$ is increasing for $\lambda \geqslant 0$. Hence, there exists a unique non-negative value of $\lambda$ such that $\lambda\sqrt{p_{\lfloor s/2\rfloor}(\lambda)}\sqrt{p_{\lceil s/2\rceil}(\lambda)} = 1$. Such a value depends only on $s$, is always comprised between 0 and 1, and decreases as $s$ increases. When $s \to \infty$, $\lambda \cdot \sqrt{p_{\lfloor s/2\rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2\rceil}(\lambda)} \approx \lambda + \lambda^3 + \cdots + \lambda^{s-1} = \lambda/(1-\lambda^2) = 1$ if $1/\lambda$ is equal to the golden ratio, that is if $\lambda = 0.6180$ (hence $\lambda \geqslant 0.6180$ for every $s > 0$). As a consequence, also $e(s) = \frac{1}{\log(1/\lambda)}$ depends only on $s$, is decreasing in $s$ and tends to 1.4404 for $s \to \infty$. Since allowing the period $s$ to be greater or equal to the protocol length $t$ is equivalent to state that the protocol is unrestricted or non-systolic, as a corollary for $s \to \infty$, it is then possible to get a lower bound differing only $O(\log\log(n))$ from the general one proved in [4,17,15,26].

Some numerical estimations for $e(s)$ arising from Corollary 4.4 are listed in Fig. 4.

## 5. Lower bounds for specific topologies

If more information about the topology of the network is known, by refining the above technique tighter bounds can be determined. For instance, this is possible for families of digraphs admitting good separators.

**Theorem 5.1.** *Let $\mathcal{G}$ be a family of digraphs having an $\langle\alpha, l\rangle$-separator and let $\langle A_1, \ldots, A_t\rangle$ be an s-systolic gossip protocol for a digraph $G = (V, A) \in \mathcal{G}$. Then $t \geqslant e(s)\log(n)(1 - o(1))$, where $e(s) = \max_{\lambda \mid 0<\lambda<1, \lambda\cdot\sqrt{p_{\lfloor s/2\rfloor}(\lambda)}\cdot\sqrt{p_{\lceil s/2\rceil}(\lambda)}\leqslant 1} l\frac{\alpha-\log\left(\lambda\cdot\sqrt{p_{\lfloor s/2\rfloor}(\lambda)}\cdot\sqrt{p_{\lceil s/2\rceil}(\lambda)}\right)}{\log(1/\lambda)}$, with $p_i(\lambda) = 1 + \lambda^2 + \cdots + \lambda^{2i-2}$ for any integer $i > 0$.*

**Proof.** Consider the delay digraph $DG = (V', A')$ and let $m = |V'| \leqslant tn/2$. Moreover, let $d = min_{x\in V_1, y\in V_2} dist_G(x, y)$ and $c = min(|V_1|, |V_2|)$, where $V_1$ and $V_2$ are the two sets associated with the $\langle\alpha, l\rangle$-separator of $G$. Without loss of generality assume $c = |V_1| \leqslant |V_2|$.

Similarly as in the proof of Theorem 4.1, there exists an $m \times m$ boolean matrix $N$ satisfying the following conditions:

- for any two vertices $x \in V_1$ and $z \in V_2$ of $G$, there exist exactly two vertices $(x, y, i) \in V'$ and $(w, z, j) \in V'$ such that the corresponding element of $N$ in the row of $(x, y, i)$ and column of $(w, z, j)$ is equal 1; all the other elements are null;
- for any real number $\lambda$ such that $0 < \lambda < 1$, $M(\lambda)^{d-1} + M(\lambda)^d + \cdots + M(\lambda)^t \geqslant \lambda^t N$.

The above conditions state that for any pair of vertices $x \in V_1$ and $z \in V_2$ of $G$, there must exist two vertices $(x, y, i) \in V'$ and $(w, z, j) \in V'$ whose distance in $DG$ is at most $t$. Moreover, as $x$ and $z$ are at distance at least $d$ in $G$, any dipath in $DG$ from $(x, y, i)$ to $(w, z, j)$ contains at least $d - 1$ different arcs (and at most $t$).

By the norm properties, for every $\lambda$ such that $0 < \lambda < 1$,

$$||M(\lambda)^{d-1} + M(\lambda)^d + \cdots + M(\lambda)^t|| \geqslant ||\lambda^t N|| = \lambda^t ||N||.$$

Moreover, let $\vec{\mathrm{J}}$ be the column vector of dimension $m$ in which the $i$th element $j_i$ is equal to 1 if the $i$th column of $M(\lambda)$ corresponds to a vertex $(y, z, j) \in V'$ such that $z \in V_2$, 0 otherwise. Notice that the 1s in $N$ can be only in the columns corresponding to the 1 entries of $\vec{\mathrm{J}}$. Therefore, if $a_i$ is the number of elements equal to 1 in the $i$th row of $N$

$$||N|| = \sup_{\vec{\mathrm{X}}\in\mathbb{R}^m} \frac{|N\vec{\mathrm{X}}|}{|\vec{\mathrm{X}}|} \geqslant \frac{|N\vec{\mathrm{J}}|}{|\vec{\mathrm{J}}|} = \frac{\sqrt{\sum_{i=1}^m a_i^2}}{|\vec{\mathrm{J}}|}$$

$$\geqslant \frac{\sqrt{\sum_{i=1}^{t\cdot c}(c/t)^2}}{\sqrt{t\cdot c}} = \frac{\sqrt{t\cdot c\cdot(c^2/t^2)}}{\sqrt{t\cdot c}} = \frac{c}{t},$$

since there are at most $t \cdot c$ entries equal to 1 in $\vec{\mathrm{J}}$ and at least $c^2$ entries equal 1 in $N$, distributed on at most $t \cdot c$ rows ($t$ per vertex in $V_1$).

Thus,

$$||M(\lambda)||^{d-1} + ||M(\lambda)||^d + \cdots + ||M(\lambda)||^t \geqslant ||M(\lambda)^{d-1}|| + ||M(\lambda)^d|| + \cdots + ||M(\lambda)^t||$$
$$\geqslant ||M(\lambda)^{d-1} + M(\lambda)^d + \cdots + M(\lambda)^t|| \geqslant \lambda^t\frac{c}{t}.$$

By Lemma 4.3, $||M(\lambda)|| \leqslant \lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)}$. Thus, for any $\lambda$ such that $0 < \lambda < 1$ and $\lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)} \leqslant 1$,

$$(t-d+2)||M(\lambda)||^{d-1} \geqslant ||M(\lambda)||^{d-1} + ||M(\lambda)||^{d} + \cdots + ||M(\lambda)||^{t} \geqslant \lambda^t c/t,$$

that is

$$\begin{aligned} t &\geqslant \frac{\log(c) - (d-1)\log(||M(\lambda)||) - \log(t-d+2) - \log(t)}{\log(1/\lambda)} \\ &\geqslant \frac{\log(c) - (d-1)\log\left(\lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)}\right) - \log(t-d+2) - \log(t)}{\log(1/\lambda)} \\ &\geqslant \frac{\alpha l \log(n) - l\log(n)\log\left(\lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)}\right) - \mathrm{o}(\log(n)) - \log(t-d+2) - \log(t)}{\log(1/\lambda)}. \end{aligned}$$

If $t \geqslant e(s)\log(n)$ the theorem trivially holds, otherwise as $\alpha$, $l$ and thus $e(s)$ are independent of $n$,

$$\begin{aligned} t &\geqslant l\frac{\alpha - \log\left(\lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)}\right)}{\log(1/\lambda)}\log(n) - \frac{\mathrm{o}(\log(n)) + 2\log(e(s)\log(n))}{\log(1/\lambda)} \\ &= l\frac{\alpha - \log\left(\lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)}\right)}{\log(1/\lambda)}\log(n)(1 - \mathrm{o}(1)). \end{aligned}$$

The theorem then follows by observing that such inequality holds for every $\lambda$ such that $0 < \lambda < 1$ and $\lambda \cdot \sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)} \leqslant 1$. □

By applying Theorem 5.1 and Lemma 3.1, the lower bounds for Butterfly, de Bruijn, and Kautz networks stated in Corollary 4.4 can be refined as follows.

**Corollary 5.2.** *The lower bounds on the gossiping time of s-systolic gossip protocols for* $BF(d,D)$, $\vec{WBF}(d,D)$, $WBF(d,D)$, $DB(d,D)$, *and* $K(d,D)$ *in Fig. 5 hold.*

Notice that in Fig. 5 we have drawn the values of $e(s)$ only for $s \leqslant 8$, but corresponding values for higher systolic periods can be determined as well. However, for $s > 8$ such values decrease slightly and only of at most 2 units starting from the second decimal digit. This can be easily verified looking at the extremal case $s = \infty$ in Fig. 6. Moreover, as it might be expected, the lower the period is with respect to the degree, the more values approach to those corresponding to any network in Fig. 4. For some of the unlisted cases with higher degree ($d = 4$ or $d = 5$) there is in fact a slight improvement for $s > 8$.

Notice that, similarly to the previous section, $e(s)$ does not depend on $n$, but only on $s$, $\alpha$ and $l$. Moreover, once fixed $\alpha$ and $l$, $e(s)$ is decreasing in $s$.

Differently from the general case, as a corollary for $s \to \infty$, for specific networks it is also possible to improve the known lower bounds on the length of non-systolic protocols.

**Corollary 5.3.** *The lower bounds on the gossiping time of any (non-systolic) gossip protocol for* $BF(d,D)$, $\vec{WBF}(d,D)$, $WBF(d,D)$, $DB(d,D)$ *and* $K(d,D)$ *in Fig. 6 hold.*

| period $s$ | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|
| $e(s)$ for $BF(2,D)$ and $W\vec{B}F(2,D)$ | 2.4401 | 2.4291 | 2.4208 | 2.4201 | 2.4194 |
| $e(s)$ for $BF(3,D)$ and $W\vec{B}F(3,D)$ | 1.8636 | 1.8136 | 1.7869 | 1.7833 | 1.7800 |
| $e(s)$ for $BF(4,D)$ and $W\vec{B}F(4,D)$ | 1.8133 * | 1.6660 | 1.6084 | 1.5991 | 1.5915 |
| $e(s)$ for $BF(5,D)$ and $W\vec{B}F(2,D)$ | 1.8133 * | 1.6502 * | 1.5469 | 1.5282 | 1.5144 |

| period $s$ | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|
| $e(s)$ for $WBF(2,D)$ | 2.0218 | 1.9959 | 1.9792 | 1.9773 | 1.9755 |
| $e(s)$ for $WBF(3,D)$ | 1.8133 * | 1.6525 | 1.5803 | 1.5684 | 1.5590 |
| $e(s)$ for $WBF(4,D)$ | 1.8133 * | 1.6502 * | 1.5363 * | 1.5022 | 1.4766 |

| period $s$ | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|
| $e(s)$ for $DB(2,D)$ and $K(2,D)$ | 1.8133 * | 1.6660 | 1.6084 | 1.5991 | 1.5915 |

Fig. 5. Some lower bounds for specific networks in the half-duplex mode. $t \geqslant e(s)\log(n)(1-o(1))$. The unlisted cases and the entries with $*$ coincide with those in Fig. 4.

| period $\infty$ | ours | previous |
|---|---|---|
| $g(BF(2,D))$ | 2.4193 | 2 (diam.) |
| $g(BF(3,D))$ | 1.7788 | 1.4404 [4,17,15,26] |
| $g(BF(4,D))$ | 1.5876 | 1.4404 [4,17,15,26] |
| $g(BF(5,D))$ | 1.5060 | 1.4404 [4,17,15,26] |
| $g(W\vec{B}F(2,D))$ | 2.4193 | 2 (diam.) |
| $g(W\vec{B}F(3,D))$ | 1.7788 | 1.4404 [4,17,15,26] |
| $g(W\vec{B}F(4,D))$ | 1.5876 | 1.4404 [4,17,15,26] |
| $g(W\vec{B}F(5,D))$ | 1.5060 | 1.4404 [4,17,15,26] |
| $g(WBF(2,D)$ | 1.9750 | 1.7621 [23] |
| $g(WBF(3,D))$ | 1.5538 | 1.4404 [4,17,15,26] |
| $g(WBF(4,D))$ | 1.4589 | 1.4404 [4,17,15,26] |
| $g(DB(2,D))$ | 1.5876 | 1.4404 [4,17,15,26] |
| $g(K(2,D))$ | 1.5876 | 1.4404 [4,17,15,26] |

Fig. 6. Some lower bounds for specific networks in the half-duplex mode. Values have to be multiplied times $\log(n)(1-o(1))$. The unlisted entries coincide with the 1.4404 of [4,17,15,26], "diam." stands for diameter.

## 6. The full-duplex case

We now briefly discuss the full-duplex case. In this case our lower bound technique can be used as well, but the norm of the matrix associated with the protocol is different. In fact, at each vertex in each round an incoming arc is activated together with the opposite arc leaving the vertex. This means that every left activation has a delay with the $s-1$ right activations belonging to the next $s-1$ rounds. Thus, if rows and columns of $M_x(\lambda)$ are both permuted in order of round, then $M_x(\lambda)$

$$\begin{vmatrix} \lambda & \lambda^2 & \lambda^3 & 0 & 0 & 0 & 0 & \cdots \\ 0 & \lambda & \lambda^2 & \lambda^3 & 0 & 0 & 0 & \cdots \\ 0 & 0 & \lambda & \lambda^2 & \lambda^3 & 0 & 0 & \cdots \\ 0 & 0 & 0 & \lambda & \lambda^2 & \lambda^3 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \lambda & \lambda^2 & \lambda^3 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \end{vmatrix}$$

Fig. 7. Example of $M_x(\lambda)$ with $s = 4$.

is such that at each row $j$ all the entries are equal to 0, except the $s-1$ ones from column $j$ to column $j+s-2$, which are respectively $\lambda, \lambda^2, \ldots, \lambda^{s-1}$ (see Fig. 7).

Then, the following lemma can be derived directly from the construction of $M_x(\lambda)$.

**Lemma 6.1.** $||M(\lambda)|| \leqslant \lambda + \lambda^2 + \cdots + \lambda^{s-1}$.

**Proof.** Let $\vec{\mathrm{E}}$ be the $t$ components column vector whose elements are all equal to 1. Then $\vec{\mathrm{E}}$ is a semi-eigenvector both of $M_x(\lambda)$ and $M_x(\lambda)^{\mathrm{T}}$ with semi-eigenvalue $\lambda + \lambda^2 + \cdots + \lambda^{s-1}$.

Thus, $\vec{\mathrm{E}}$ is a semi-eigenvector of $M_x(\lambda)^{\mathrm{T}} M_x(\lambda)$ with semi-eigenvalue $(\lambda + \lambda^2 + \cdots + \lambda^{s-1})^2$, as $M_x(\lambda)^{\mathrm{T}} M_x(\lambda)\vec{\mathrm{E}} \leqslant M_x(\lambda)^{\mathrm{T}}(\lambda + \lambda^2 + \cdots + \lambda^{s-1})\vec{\mathrm{E}} \leqslant (\lambda + \lambda^2 + \cdots + \lambda^{s-1})^2\vec{\mathrm{E}}$.

By Lemma 2.1,

$||M(\lambda)|| = \sqrt{\rho(M_x(\lambda)^{\mathrm{T}} M_x(\lambda))} \leqslant \lambda + \lambda^2 + \cdots + \lambda^{s-1}$. □

As a corollary of Theorem 4.1, any $s$-systolic gossip protocol has length $t \geqslant e(s)\log(n) - \mathrm{O}(\log\log(n))$, where $n = |V|$, $e(s) = 1/\log(1/\lambda)$ and $\lambda$ is the real positive number such that $0 < \lambda < 1$ and $\lambda + \lambda^2 + \cdots \lambda^{s-1} = 1$. Unfortunately, this does not improve with respect to the previous results, since it coincides with the lower bound that can be inferred directly from broadcasting. In fact, a full-duplex $s$-systolic gossip protocol for a symmetric digraph $G$ can be easily transformed into a broadcast protocol for a $d$-bounded degree network, so that a lower bound on the broadcasting time in $d$-bounded degree networks is also a lower bound on the gossiping time of $s$-systolic full-duplex protocols (see [8]).

| period $s$ | 3 | 4 | 5 | 6 | 7 | $\infty$ | previous |
|---|---|---|---|---|---|---|---|
| $e(s)$ for $BF(2,D)$ | 2.2200 | 2.2104 | 2.2097 | 2.2096 | 2.2096 | 2.2096 | 2 (diam.) |
| $e(s)$ for $BF(3,D)$ | 1.5627 | 1.5244 | 1.5209 | 1.5204 | 1.5203 | 1.5203 | 1.2618 (diam.) |
| $e(s)$ for $BF(4,D)$ | 1.4404 * | 1.3042 | 1.2957 | 1.2942 | 1.2939 | 1.2938 | 1.0058 [22,2] |
| $e(s)$ for $BF(5,D)$ | 1.4404 * | 1.2041 | 1.1879 | 1.1847 | 1.1839 | 1.1837 | 1.0014 [22,2] |
| $e(s)$ for $WBF(4,D)$ | 1.4404 * | 1.1463 | 1.1133 | 1.1069 | 1.1052 | 1.1044 | 1.0058 [22,2] |
| $e(s)$ for $WBF(5,D)$ | 1.4404 * | 1.1374 * | 1.0642 | 1.0496 | 1.0454 | 1.0432 | 1.0014 [22,2] |
| $e(s)$ for $K(2,D)$ | 1.4404 * | 1.3042 | 1.2957 | 1.2942 | 1.2939 | 1.2938 | 1.1374 [22,2] |
| $e(s)$ for $K(3,D)$ | 1.4404 * | 1.1374 * | 1.0602 | 1.0433 | 1.0384 | 1.0358 | 1.0254 [22,2] |

Fig. 8. Some lower bounds in the full-duplex mode. $t \geqslant e(s)\log(n)(1 - \mathrm{o}(1))$. The unlisted cases and the entries with $*$ coincide with those in [22,2]. For $WBF(d,D)$ and $DB(d,D)$ with $d = 2, 3$ better results have been derived in [23].

However, for networks having good separators it is possible to obtain lower bounds that improve with respect to the previous ones and, when no nontrivial lower bound is known, with respect to the diameter (recall that the diameter is a lower bound as there are items that have to travel paths of length equal to the diameter). In fact, by exploiting the same arguments of Theorem 5.1, it is possible to show that any $s$-systolic gossip protocol in the full-duplex case for a network with an $\langle \alpha, l \rangle$-separator has length $t \geqslant e(s)\log(n) - o(\log(n))$, where $e(s) = \max_{\lambda \mid 0<\lambda<1, \lambda+\lambda^2+\cdots+\lambda^{s-1} \leqslant 1} l\left(\frac{\alpha - \log(\lambda+\lambda^2+\cdots+\lambda^{s-1})}{\log(1/\lambda)}\right)$.

New lower bounds can thus be determined for many networks, although in Fig. 8 we give examples only for some $BF(d,D)$, $WBF(d,D)$ and $K(d,D)$. Again, as a limit for $s \to \infty$, our results improve also with respect to non-systolic protocols.

Like in the half-duplex case, as it might be expected the lower the period is with respect to the degree, the more values approach to those corresponding to the general case, which coincide to the ones inferred from broadcasting in [22,2].

## 7. Conclusion

In this paper we have provided an innovative and powerful technique allowing to considerably improve the previous lower bounds on the gossiping time.

In fact, we have proved new lower bounds on systolic gossip for general networks in the directed and half-duplex cases. In this setting, no general result was previously known. Moreover, as a corollary for $s \to \infty$, our technique yields a lower bound only $O(\log\log(n))$ far from the general one for all graphs proved in [4,17,15,26]. In the full-duplex mode, for general networks our results differ only $O(\log\log(n))$ from the ones that come directly from broadcasting [22,2]. As recently shown in [5], all the above bounds are optimal up to an $O(\log\log(n))$ additive factor.

We have refined our technique to deal also with specific networks and we have improved the known results for Butterfly, de Bruijn, and Kautz graphs, even in the full-duplex case. Again, as a limit for $s \to \infty$, for such topologies better lower bounds have been determined even for unrestricted protocols, i.e., non-systolic.

To our opinion, the relevant contribution relies more on the introduced lower bound technique, rather than the numerical values. In fact, although we have given here only a limited number of examples, it allows to find nontrivial lower bounds also for many other interconnection networks simply by exploiting very general topological properties. This holds even in the full-duplex case and for non-systolic protocols.

Our technique can be applied also in other more general contexts as well, for instance to establish lower bounds on the diameter of weighted digraphs. Such issues have not been considered in the paper and to our opinion deserve further investigation.

## Acknowledgments

We thank Jean-Claude Bermond, Ralf Klasing, Alberto Marchetti Spaccamela, and the anonymous referees for very helpful comments.

## References


[1] A. Berman, R. Plemmons, Nonnegative matrices in the mathematical science, Classics in Applied Mathematics, SIAM, 1994..

[2] J. Bermond, P. Hell, A. Liestman, J. Peters, Broadcasting in bounded degree graphs, SIAM Journal on Discrete Mathematics 5 (1) (1992) 10–24.

[3] J. de Rumeur, Communication dans les réseaux de processeurs, Collection Etudes et Recherches en Informatique, Masson, 1994 (English version to appear).

[4] S. Even, B. Monien, On the number of rounds necessary to disseminate information, in: Proc. 1st ACM Symposium on Parallel Algorithms and Architectures (SPAA), 1989, pp. 318–327..

[5] M. Flammini, S. Pérennès, On the optimality of general lower bounds for broadcasting and gossiping, SIAM Journal on Discrete Mathematics 14 (2) (2001) 267–282.

[6] P. Fraigniaud, E. Lazard, Methods and problems of communication in usual networks, Discrete Applied Mathematics 53 (1–3) (1994) 79–133.

[7] S. Hedetniemi, S. Hedetniemi, A. Liestman, A survey of gossiping and broadcasting in communication networks, Networks 18 (1986) 319–349.

[8] J. Hromkovič, R. Klasing, D. Pardubská, W. Unger, H. Wagener, The complexity of systolic dissemination of information in interconnection networks, R.A.I.R.O. Theoretical Informatics and Applications 28 (3–4) (1994) 303–342.

[9] J. Hromkovič, R. Klasing, B. Monien, R. Peine, Dissemination of information in interconnection networks (broadcasting and gossiping), in: Ding-Zhu Du, D. Frank Hsu (Eds.), Combinatorial Network Theory, Kluwer Academic Publishers, 1995, pp. 125–212.

[10] J. Hromkovič, R. Klasing, E. Stohr, H. Wagener, Gossiping in vertex-disjoint paths mode in d-dimensional grids and planar graphs, Information and Computation 123 (1) (1995) 17–28.

[11] J. Hromkovič, R. Klasing, D. Pardubská, W. Unger, J. Waczulik, H. Wagener, Effective systolic algorithms for gossiping in cycles and two-dimensional grids, in: Proc. 10th Conference on Fundamentals of Computation Theory (FCT), Vol. 965 of Lecture Notes in Computer Science, Springer-Verlag, 1995, pp. 273–282.

[12] J. Hromkovič, R. Klasing, W. Unger, H. Wagener, Optimal algorithms for broadcast and gossip in the edge-disjoint path modes, Information and Computation 133 (1) (1997) 1–33.

[13] R. Klasing, B. Monien, R. Peine, E. Stohr, Broadcasting in butterfly and de Bruijn networks, Discrete Applied Mathematics 53 (1–3) (1994) 183–197.

[14] G. Kortsarz, D. Peleg, Traffic-light scheduling on the grid, Discrete Applied Mathematics 53 (1–3) (1994) 211–234.

[15] D.W. Krumme, G. Cybenko, K.N. Venkataraman, Gossiping in minimal time, SIAM Journal on Computing 21 (1) (1992) 111–139.

[16] H. Kung, Let's design algorithms for VLSI systems, in: C.L.L. Seifz (Ed.), Proceedings of the Caltech Conference of VLSI, Pasadena, California, 1979, pp. 65–90.

[17] R. Labahn, I. Warnke, Quick gossiping by multi-telegraphs, Topics in Combinatorics and Graph Theory (1990) 451–458.

[18] R. Labahn, S. Hedetniemi, R. Laskar, Periodic gossiping on trees, Discrete Applied Mathematics 53 (1–3) (1994) 235–246.

[19] T. Leighton, Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes, Morgan Kaufman, 1992.

[20] A. Liestman, D. Richards, Network communication in edge-colored graphs: gossiping, IEEE Transactions on Parallel and Distributed Systems 4 (1993) 438–445.

[21] A. Liestman, D. Richards, Perpetual gossiping, Parallel Processing Letters 3 (4) (1993) 347–355.

[22] A. Liestman, J. Peters, Broadcast networks of bounded degree, SIAM Journal on Discrete Mathematics 1 (4) (1998) 531–540.

[23] S. Pérennès, Lower bounds on broadcasting time of de Bruijn networks, in: Proc. 2nd Int. Euro-Par Conference, Vol. 1123 of Lecture Notes in Computer Science, Springer-Verlag, 1996, pp. 325–332.

[24] S. Pérennès, Communications dans les réseaux d'interconnexion, Ph.D. thesis, Université de Nice—Sophia Antipolis, Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis CNRS URA 1376, 1996.

[25] S. Pérennès, Broadcasting and gossiping on de Bruijn, shuffle-exchange and similar networks, Discrete Applied Mathematics 83 (1998) 247–262.
[26] V. Sunderam, P. Winkler, Fast information sharing in a complete network, Discrete Applied Mathematics 42 (1993) 75–86.